Counting Points on Curves using Monsky-Washnitzer Cohomology

Frederik Vercauteren
frederik@cs.bris.ac.uk

Jan Denef
jan.denef@wis.kuleuven.ac.be

University of Leuven
http://www.arehcc.com
University of Bristol
Overview

- “Who’s who” of $p$-adic point counting
- Zeta functions and Weil conjectures
- Monsky-Washnitzer cohomology
- Kedlaya’s algorithm for hyperelliptic curves in odd characteristic
- Extending Kedlaya’s algorithm to $C_{a,b}$ curves
- Experimental results
- Conclusions and open problems
## “Who’s who” of $p$-adic point counting

<table>
<thead>
<tr>
<th>Elliptic Curves over $\mathbb{F}_{p^n}$</th>
<th>$p$</th>
<th>Time</th>
<th>Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satoh</td>
<td>$p \geq 5$</td>
<td>$O(n^{3+\varepsilon})$</td>
<td>$O(n^3)$</td>
</tr>
<tr>
<td>Skjernaa</td>
<td>$p = 2$</td>
<td>$O(n^{3+\varepsilon})$</td>
<td>$O(n^3)$</td>
</tr>
<tr>
<td>Fouquet-Gaudry-Harley</td>
<td>$p = 2, 3$</td>
<td>$O(n^{3+\varepsilon})$</td>
<td>$O(n^3)$</td>
</tr>
<tr>
<td>Vercauteren</td>
<td>all $p$</td>
<td>$O(n^{3+\varepsilon})$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Mestre-Harley (AGM)</td>
<td>$p = 2$</td>
<td>$O(n^{3+\varepsilon})$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Satoh-Skjernaa-Taguchi</td>
<td>all $p$</td>
<td>$O(n^{2+1/2+\varepsilon})$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Gaudry</td>
<td>$p = 2$</td>
<td>$O(n^{2+1/2+\varepsilon})$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Carls</td>
<td>all $p$</td>
<td>$O(n^{3+\varepsilon})$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Harley</td>
<td>all $p$</td>
<td>$O(n^{2+1/2+\varepsilon})$</td>
<td>$O(n^2)$</td>
</tr>
<tr>
<td>Mestre-Lercier-Lubicz</td>
<td>all $p$</td>
<td>$O(n^{2+\varepsilon})$</td>
<td>$O(n^2)$</td>
</tr>
</tbody>
</table>
### “Who’s who” of $p$-adic point counting

<table>
<thead>
<tr>
<th>Hyperelliptic curves over $\mathbb{F}_{p^n}$</th>
<th>$p$</th>
<th>Time</th>
<th>Space</th>
<th>Genus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kedlaya</td>
<td>$p \geq 3$</td>
<td>$O(g^{4+\varepsilon} n^{3+\varepsilon})$</td>
<td>$O(g^3 n^3)$</td>
<td>all $g$</td>
</tr>
<tr>
<td>Mestre-Gaudry-Harley</td>
<td>$p = 2$</td>
<td>$O(n^{3+\varepsilon})$</td>
<td>$O(n^2)$</td>
<td>$g = 2$ (O)</td>
</tr>
<tr>
<td>Lauder-Wan</td>
<td>all $p$</td>
<td>$O(g^{5+\varepsilon} n^{3+\varepsilon})$</td>
<td>$O(g^3 n^3)$</td>
<td>all $g$ (AS)</td>
</tr>
<tr>
<td>Denef-Vercauteren</td>
<td>$p = 2$</td>
<td>$O(g^{4+\varepsilon} n^{3+\varepsilon})$</td>
<td>$O(g^3 n^3)$</td>
<td>all $g$</td>
</tr>
<tr>
<td>Mestre-Lercier-Lubicz</td>
<td>$p = 2$</td>
<td>$O(2^g n^{2+\varepsilon})$</td>
<td>$O(2^g n^2)$</td>
<td>$g = 2$ (O)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Superelliptic curves over $\mathbb{F}_{p^n}$</th>
<th>$p$</th>
<th>Time</th>
<th>Space</th>
<th>Genus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaudry-Gürel</td>
<td>all $p$</td>
<td>$O(g^{4+\varepsilon} n^{3+\varepsilon})$</td>
<td>$O(g^3 n^3)$</td>
<td>all $g$</td>
</tr>
<tr>
<td>Lauder</td>
<td>all $p$</td>
<td>$O(g^{4+\varepsilon} n^{3+\varepsilon})$</td>
<td>$O(g^3 n^3)$</td>
<td>$a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$C_{a,b}$ curves over $\mathbb{F}_{p^n}$</th>
<th>$p$</th>
<th>Time</th>
<th>Space</th>
<th>Genus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denef-Vercauteren</td>
<td>all $p$</td>
<td>$O(g^3+\varepsilon n^{3+\varepsilon})$</td>
<td>$O(g^3 n^3)$</td>
<td>all $g$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Algebraic varieties over $\mathbb{F}_{p^n}$</th>
<th>$p$</th>
<th>Time</th>
<th>Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lauder-Wan</td>
<td>all $p$</td>
<td>Polynomial</td>
<td>Polynomial</td>
</tr>
</tbody>
</table>
The Zeta Function and Weil Conjectures

Let $\overline{C}$ be a smooth projective curve over $\mathbb{F}_q$, then the zeta function of $\overline{C}$ is

$$Z(t) = Z(\overline{C}; t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right)$$

with $N_r$ the number of points on $\overline{C}$ with coordinates in $\mathbb{F}_{q^r}$.

Weil Conjectures:

- $Z(t)$ is rational function over $\mathbb{Z}$ and can be written as $\frac{P(t)}{(1-t)(1-qt)}$
- $P(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$ with $g$ genus of $\overline{C}$ and $|\alpha_i| = \sqrt{q}$
- $P(t) = \sum_{i=0}^{2g} a_i t^i$ with $a_0 = 1$, $a_{2g} = q^g$ and $a_{g+i} = q^i a_{g-i}$
- $N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$ and $P(1)$ is the order of $\text{Jac}(\overline{C}/\mathbb{F}_q)$
Unramified Extensions of $p$-adics

- $K$ extension of $\mathbb{Q}_p$ of degree $n$ with valuation ring $R$ and maximal ideal $M_R = \{x \in K \mid |x|_p < 1\}$ of $R$.

- $K$ is called unramified iff its residue field $R/M_R \cong \mathbb{F}_q$.

- Let $\mathbb{F}_q \cong \mathbb{F}_p[t]/(\overline{Q}(t))$ then $K$ can be constructed as

$$K \cong \mathbb{Q}_p[t]/(Q(t)),$$

with $Q(t)$ any monic lift of $\overline{Q}(t)$ to $\mathbb{Z}_p[t]$.

- $\text{Gal}(K/\mathbb{Q}_p)$ is cyclic with generator Frobenius substitution $\sigma$ and $\sigma$ modulo $p$ equals $p$-th power Frobenius $\overline{\sigma}$ on $\mathbb{F}_q$.

- Since $q = p^n$ we have $F = \sigma^n$ and $\overline{F}$ is $q$-th power Frobenius.
Computing Zeta Function - General Strategy

- $\overline{X}$ smooth affine variety over $\mathbb{F}_q$ of dimension $d$.

- Monsky and Washnitzer construct $K$-vectorspaces $H^i(\overline{X}/K)$ with an induced action of Frobenius $F_*$ on it such that these cohomology groups satisfy a Lefschetz trace formula:

$$N_r = \sum_{i=0}^{d} (-1)^i \text{Tr} \left( (q^d F_*^{-1})^r \middle| H^i(\overline{X}/K) \right)$$

- For smooth affine curve $\overline{C}$ the only non-trivial MW cohomology groups are $H^0(\overline{C}/K)$ and $H^1(\overline{C}/K)$, so

$$\#\overline{C}(\mathbb{F}_{q^r}) = q^r - \text{Trace} \left( (q F_*^{-1})^r \middle| H^1(\overline{C}/K) \right)$$
Hyperelliptic Curves

• Hyperelliptic curve $\overline{C}$ of genus $g$ over finite field $\mathbb{F}_q$,

$$\overline{C} : y^2 + \overline{h}(x)y = \overline{f}(x)$$

where $\deg \overline{h} \leq g$, $\overline{f}$ monic, $\deg \overline{f} = 2g + 1$ and $\overline{C}$ non-singular.

• If $\text{char } \mathbb{F}_q > 2$ one can take $\overline{h} = 0$ and $\overline{f}$ has to be squarefree.

• Jacobian $\text{Jac}(\overline{C}/\mathbb{F}_q)$ is abelian group associated with $\overline{C}$ which is quotient group of degree 0 divisors by principal divisors.

• Problem: compute order of $\text{Jac}(\overline{C}/\mathbb{F}_q)$.
Kedlaya’s Algorithm - $p$ Small Odd Prime

- $\overline{C} : y^2 - \overline{f}(x) = 0$ genus $g$ affine hyperelliptic curve $\overline{C}$ over $\mathbb{F}_{p^n}$.

- Affine curve $\overline{C}'$ is $C$ minus points $(\theta_i, 0)$ for $0 \leq i \leq 2g$. Coordinate ring $\overline{A}$ of $\overline{C}'$ is $\mathbb{F}_q[x, y, y^{-1}]/(y^2 - \overline{f}(x))$.

- Take any monic lift $f(x) \in R[x]$ of $\overline{f}(x)$ and let $C'$ be affine curve $y^2 - f(x) = 0$ minus $2g + 1$ points $(\theta_i, 0)$ for $0 \leq i \leq 2g$.

- The coordinate ring of $C'$ then is $A = R[x, y, y^{-1}]/(y^2 - f(x))$.

- The weak completion or dagger ring $A^\dagger$ consists of series

$$
\sum_{k=-\infty}^{+\infty} \sum_{i=0}^{2g} a_{i,k} x^i y^k
$$

and valuation of $a_{i,k}$ grows linearly with $|k|$. 
Kedlaya’s Algorithm - Frobenius on $A^\dagger$

Lift $\sigma$ to $\sigma : A^\dagger \to A^\dagger$ as

$$x^\sigma := x^p \quad \text{and} \quad y^\sigma \text{ satisfies } (y^\sigma)^2 = f(x)^\sigma.$$ 

Formula for $y^\sigma$ as element of $A^\dagger$: 

$$y^\sigma = (f(x)^\sigma)^{1/2}$$

$$= (f(x)^\sigma - f(x)^p + f(x)^p)^{1/2}$$

$$= f(x)^{p/2}(1 + \frac{f(x)^\sigma - f(x)^p}{f(x)^p})^{1/2}$$

$$= y^{p} \sum_{k=0}^{\infty} \binom{1/2}{k} \frac{(f(x)^\sigma - f(x)^p)^k}{y^{2p^k}}$$
Kedlaya’s Algorithm - Cohomology Groups

- Let \( D^1(A^\dagger) := (A^\dagger dx + A^\dagger dy)/(2ydy - f'(x)dx) \) and
  \[
d_0 : A^\dagger \rightarrow D^1(A^\dagger) \quad \text{and} \quad d_1 : D^1(A^\dagger) \rightarrow \bigwedge^2 D^1(A^\dagger),
\]
  then \( H^0(\overline{A}/R) = \text{Ker} \, d_0 = R \) and \( H^1(\overline{A}/R) = \text{Ker} \, d_1/\text{Im} \, d_0 \).

- \( H^1(\overline{A}/K) := H^1(\overline{A}/R) \otimes_R K \) splits into eigenspaces under \( \iota \)
  - Invariant: \( H^1(\overline{A}/K)^+ \) with basis \( x^i dx/y^2 \) for \( 0 \leq i \leq 2g \)
  - Anti-invariant: \( H^1(\overline{A}/K)^- \) with basis \( x^i dx/y \) for \( 0 \leq i < 2g \)

- \( H^1(\overline{A}/K)^+ \) corresponds to the \( 2g + 1 \) removed points \((\theta_i, 0)\)

- Characteristic polynomial of \( F_* \) on \( H^1(\overline{A}/K)^- \) equals
  \[
  \chi(t) := t^{2g} P(1/t)
  \]
Kedlaya’s Algorithm - Computing Zeta Function

- The action of $\sigma_*$ on a differential form $x^k dx/y$ is given by
  \[ \sigma_*(x^k dx/y) = px^{pk+p-1} dx/y^\sigma. \]

- Use reduction formulae to express this on basis of $H^1(\overline{A}/K)^-$. 

- This gives matrix $M$ which is an approximation of the action of $\sigma_*$ on $H^1(\overline{A}/K)^-$. 

- The polynomial $\chi(t) := t^{2g} P(1/t)$ can then be approximated by the characteristic polynomial of $MM^\sigma \cdots M^{\sigma^n-1}$. 
# Kedlaya’s Algorithm - Complexity

Complexity for genus $g$ hyperelliptic curve over $\mathbb{F}_{p^n}$

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Time Complexity</th>
<th>Space Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Char $p \neq 2$: Kedlaya</td>
<td>$O(g^{4+\varepsilon}n^{3+\varepsilon})$</td>
<td>$O(g^3n^3)$</td>
</tr>
<tr>
<td>Char 2: Average case</td>
<td>$O(g^{4+\varepsilon}n^{3+\varepsilon})$</td>
<td>$O(g^3n^3)$</td>
</tr>
<tr>
<td>Char 2: Worst case</td>
<td>$O(g^{5+\varepsilon}n^{3+\varepsilon})$</td>
<td>$O(g^4n^3)$</td>
</tr>
</tbody>
</table>

- Complexity depends on splitting type of $\bar{h}(x) = \prod_{i=1}^{s}(x - \bar{\theta}_i)^{m_i}$.
- Worst case is $s \approx g/2$, $m_i = 1$ for $0 < i < s$ and $m_s \approx g/2$. 
$C_{a,b}$ CURVES

- $C_{a,b}$ curve $\overline{C}$ over finite field $\mathbb{F}_q$,

$$\overline{C} : y^a + \sum_{i=1}^{a-1} f_i(x)y^i + f_0(x) = 0$$

where $\deg f_0(x) = b$, $a \deg f_i(x) + bi \leq ab$ and $\gcd(a, b) = 1$.

- Absolutely irreducible and if smooth genus is $g = \frac{(a-1)(b-1)}{2}$.

- Unique degree 1 place $Q$ at infinity and $v_Q(x) = -a$, $v_Q(y) = -b$.

- Various subclasses of $C_{a,b}$ curves:
  - Hyperelliptic curves: $a = 2$ and $b = 2g + 1$
  - Superelliptic curves: $f_i(x) = 0$ for $i = 1, \ldots, a - 1$
$C_{a,b}$ curves - Lift of Curve

- The affine curve $\overline{C}$ has coordinate ring $\overline{A} := \mathbb{F}_q[x, y]/(\overline{C})$.

- Take arbitrary lifts $f_i(x) \in R[x]$ of $\overline{f}_i(x)$ for $i = 0, \ldots, a - 1$ with $\deg f_i(x) = \deg \overline{f}_i(x)$ and define

$$C : y^a + \sum_{i=1}^{a-1} f_i(x)y^i + f_0(x) = 0$$

- Let $A^\dagger$ be the dagger ring of $A := R[x, y]/(C)$.

- Elements of $A^\dagger$ can be represented as $\sum_{l=0}^{a-1} \sum_{k=0}^{+\infty} a_{k,l} x^k y^l$ and the valuation of $a_{k,l}$ grows linearly with $k$. 
\( \mathcal{C}_{a,b} \text{ CURVES - FROBENIUS on } A^\dagger \)

- The necessary conditions on the Frobenius \( \sigma \) on \( A^\dagger \) are

\[
x^\sigma \equiv x^p \mod p \quad \text{and} \quad y^\sigma \equiv y^p \mod p \quad \text{and} \quad C^\sigma(x^\sigma, y^\sigma) = 0
\]

- Fixing \( x^\sigma = x^p \) also fixes \( y^\sigma \) as the solution of \( C^\sigma(x^p, y^\sigma) = 0 \), which implies that \( \left( \frac{\partial C(x, y)}{\partial y} \right)^p \) has to be invertible in \( A^\dagger \).

- **Main idea:** lift Frobenius on \( x \) and \( y \) simultaneously such that denominator in the Newton iteration is invertible in \( A^\dagger \).

- Let \( Z \in A^\dagger \) such that \( x^\sigma = x^p + \alpha Z \) and \( y^\sigma = y^p + \beta Z \), then

\[
C^\sigma(x^\sigma, y^\sigma) = C^\sigma(x^p + \alpha Z, y^p + \beta Z) = 0 \quad \text{and} \quad Z \equiv 0 \mod p
\]
$C_{a,b}$ CURVES - FROBENIUS ON $A^\dagger$

- Let $G(Z) := C^\sigma(x^p + \alpha Z, y^p + \beta Z)$, then $Z_{k+1} = Z_k - \frac{G(Z_k)}{G'(Z_k)}$ with

$$G'(Z) \equiv \alpha \frac{\partial C^\sigma}{\partial x} \big|_{(x^p,y^p)} + \beta \frac{\partial C^\sigma}{\partial y} \big|_{(x^p,y^p)} + O(Z) \mod p$$

- $G'(Z)$ will be invertible in $A^\dagger$ if $G'(Z) \equiv 1 \mod p$ and thus

$$G'(Z) \equiv \alpha \left( \frac{\partial C}{\partial x} \right)^p + \beta \left( \frac{\partial C}{\partial y} \right)^p \equiv 1 \mod p$$

- Assume $\overline{C}$ non-singular, then $\frac{\partial \overline{C}}{\partial x}, \frac{\partial \overline{C}}{\partial y}$ and $\overline{C}$ generate unit ideal and using Buchberger’s algorithm we compute $\overline{\alpha}, \overline{\beta}, \overline{\gamma} \in \overline{A}$ with

$$1 = \overline{\alpha} \left( \frac{\partial \overline{C}}{\partial x} \right)^p + \overline{\beta} \left( \frac{\partial \overline{C}}{\partial y} \right)^p + \overline{\gamma} \overline{C}$$
\( C_{a,b} \) CURVES - BASIS OF \( H^1(\overline{A}/K) \)

- If \( \overline{C} \) is smooth, then \( 2g = (a - 1)(b - 1) \) and a basis for \( H^1(\overline{A}/K) \)

\[ x^k y^l \, dx \quad \text{for} \quad k = 0, \ldots, b - 2 \text{ and } l = 1, \ldots, a - 1 \]

- Using equation of the curve: \( x^i y^l \, dx \) or \( x^i y^l \, dy \) for \( 0 \leq l < a \)

- Clearly \( d(x^i y^{l+1}) \equiv 0 \) and thus \( x^i y^l \, dy \equiv -\frac{1}{l+1} x^{i-1} y^l \, dx \)

- Differentiating the curve \( C \) leads to the equality

\[
\sum_{i=1}^{a-1} \left( \frac{f'_i(x) y^i + f'_0(x)}{i} \right) \, dx = -(ay^{a-1} + \sum_{i=1}^{a-1} f_i(x) iy^{i-1}) \, dy
\]
\textbf{\textit{C}_{a,b} \textit{curves - Reduction Formula}}

- To reduce $x^iy^l \, dx$ we multiply this equation with $x^jy^l$

\[ x^j\left(\sum_{i=1}^{a-1} f'_i(x)y^i + f'_0(x)\right)y^l \, dx = -x^j(ay^{a-1} + \sum_{i=1}^{a-1} f_i(x)i y^{i-1})y^l \, dy \]

\(*\)

- Partially integrating the right-hand side to $y$ gives

\[ d\left(x^j \left( \frac{a}{a+1}y^{a+l} + \sum_{i=1}^{a-1} \frac{i}{i+l} f_i(x)y^{i+l} \right) \right) \equiv 0 \]

- This gives an expression for the right-hand side of (*) and thus

\[ x^j \left( \sum_{i=1}^{a-1} \frac{l}{i+l} f'_i(x)y^i + f'_0(x) \right) y^l \, dx \equiv jx^{j-1} \left( \frac{a}{a+l}y^a + \sum_{i=1}^{a-1} \frac{i}{i+l} f_i(x)y^i \right) y^l \, dx \]
The action of $\sigma_*$ on a differential form $x^k y^l dx$ is given by

$$\sigma_*(x^k y^l dx) \equiv (x^\sigma)^k (y^\sigma)^l \; dx^\sigma.$$ 

Substituting power series for $x^\sigma$ and $y^\sigma$, we can write $\sigma_*(x^k y^l dx)$ on basis of $H^1(\overline{A}/K)$ using the reduction formulae.

This gives matrix $M$ which is an approximation of the action of $\sigma_*$ on $H^1(\overline{A}/K)$.

The polynomial $\chi(t) := t^{2g} P(1/t)$ can then be approximated by the characteristic polynomial of $M M^\sigma \cdots M^{\sigma^{n-1}}$. 

$C_{a,b}$-curves - Zeta Function
**Dependence on size of Jacobian**

Timings for 180-bit Jacobians of hyperelliptic curves for various genus $g$ and extension degrees $n$.

<table>
<thead>
<tr>
<th>Genus $g$</th>
<th>Degree $n$</th>
<th>Lifting $y^\sigma$ (s)</th>
<th>Reduction (s)</th>
<th>Total (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>90</td>
<td>64</td>
<td>19</td>
<td>86</td>
</tr>
<tr>
<td>3</td>
<td>60</td>
<td>78</td>
<td>27</td>
<td>106</td>
</tr>
<tr>
<td>4</td>
<td>45</td>
<td>76</td>
<td>36</td>
<td>114</td>
</tr>
<tr>
<td>5</td>
<td>36</td>
<td>93</td>
<td>45</td>
<td>139</td>
</tr>
<tr>
<td>10</td>
<td>18</td>
<td>193</td>
<td>137</td>
<td>334</td>
</tr>
<tr>
<td>15</td>
<td>12</td>
<td>210</td>
<td>247</td>
<td>460</td>
</tr>
<tr>
<td>20</td>
<td>9</td>
<td>344</td>
<td>413</td>
<td>762</td>
</tr>
</tbody>
</table>
Kedlaya in Char 2 - Example: Genus 3 over $\mathbb{F}_{2^{59}}$

Let $\mathbb{F}_{2^{59}}$ be defined as $\mathbb{F}_2[t]/\overline{P}(t)$ with $\overline{P}(t) = t^{59} + t^7 + t^4 + t^2 + 1$ and consider the random hyperelliptic curve $C_3$ of genus 3 defined by

$$y^2 + (\sum_{i=0}^{3} h_i x^i) y = x^7 + \sum_{i=0}^{6} f_i x^i,$$

where

$h_0 = 569121E97EB3821$  \quad h_1 = 49F340F25EA38A2$  \quad h_2 = 2DE854D48D56154$  \quad h_3 = 0B6372FF7310443$

$f_0 = 1104FDBEB454C58$  \quad f_1 = 0C426890E5C7481$  \quad f_2 = 34967E2EB7D50C3$  \quad f_3 = 1F1728AA28C616C$

$f_4 = 1AE177BFE49826A$  \quad f_5 = 3895A0E400F7D18$  \quad f_6 = 6DF634A1E2BFA8E$

The group order of the Jacobian $J_{\tilde{C}_3}$ of $C_3$ over $\mathbb{F}_{2^{59}}$ is

$$\#J_{\tilde{C}_3} = 2 \cdot 95780971407243394633762332360123160334059170481903949$$

where the last factor is 176-bit prime.
Conclusions & Open Problems

• Now possible to compute the zeta function of hyperelliptic curves and $C_{a,b}$ curves over finite fields of any small characteristic.

• Complexity: $O(g^{4+\varepsilon}n^{3+\varepsilon})$ operations and $O(g^{3}n^{3})$ space.

• Resulting algorithms can be used to generate curves suitable for cryptography, but not as fast as AGM.

• Can we get substantial improvement for ordinary curves?

• Lifting works for arbitrary non-singular affine curves, but how easy is it to write down explicit basis and reduction formulae?

• Golden grail: practical algorithms for large $p$?