Shimura curves and bilinear multiplication algorithms in finite fields

Matthieu Rambaud

Telecom ParisTech

Sep 2nd, 2017

Contents of the talk

Executive summary

Symmetric bilinear complexity in $\mathbf{F}_{p^n}/\mathbf{F}_p$

$$\mathbf{F}_{p^n} \times \mathbf{F}_{p^n} \longrightarrow \mathbf{F}_{p^n}$$

$$m : (x, y) \longrightarrow x \cdot y = \sum_{i=1}^{\mu_p^{\mathrm{sym}}(n)} \phi_i(x) \bullet \phi_i(y) \cdot w_i \; (\phi_i \in \mathbf{F}^*_{p^n}, w_i \in \mathbf{F}_{p^n})$$

Executive summary

Symmetric bilinear complexity in $\mathbf{F}_{p^n}/\mathbf{F}_p$

$$\mathbf{F}_{p^n} \times \mathbf{F}_{p^n} \longrightarrow \mathbf{F}_{p^n}$$

$$m : (x, y) \longrightarrow x \cdot y = \sum_{i=1}^{\mu_p^{\mathrm{sym}}(n)} \phi_i(x) \bullet \phi_i(y) \cdot w_i \; (\phi_i \in \mathbf{F}_{p^n}^*, w_i \in \mathbf{F}_{p^n})$$

Goal: upper bound $M_p^{\mathrm{sym}} = \limsup_{n \to \infty} \frac{1}{n} \mu_p^{\mathrm{sym}}(n)$

p	Before	This work	under Conj. Y (solved since)
2	15.2	**10**	6.92
3	7.73	**5.42**	5.39

Strategy for bilinear multiplication

f and g in $\mathbf{F}_p[X]$ of degree n, compute $f \cdot g$

1. *Choose* $P_1, \ldots, P_{2n+1}$ in $\mathbf{F}_p$.
2. *Evaluate* $f(P_i)_{i=1..2n+1}$ and $g(P_i)_{i=1..2n+1}$.
3. *Compute* $\left\{f \cdot g(P_i) = f(P_i) \bullet g(P_i)\right\}_i$: $2n+1$ multiplications.
4. *Lagrange's interpolation:* recover $f \cdot g$.

Chudnovky^2's improvement

	Before	After
set:	$\mathbf{F}_p$	curve $X_{/\mathbf{F}_p}$
f and g in $\mathbf{F}_p[X]$:	polynomials	rational functions f and g in $\mathcal{L}(D)$
evaluation on:	points $P_1, \ldots P_{2n+1}$ in $\mathbf{F}_p$	points $P_1, \ldots P_{2n+\mathbf{g}+1}$ in $X(\mathbf{F}_p)$

Contents of the thesis

- Theorem A: fixes and improves all state of the art upper-bounds.
- Theorem B: improves the choice of the curve.
- On a fixed curve: construction and optimisation of the algorithm.

the Graal: Conjecture Y

Conjecture

Let p be a prime and $2t \geqslant 2$. Does there exist a family $(X_s)_{s\geqslant 1}$ of curves, with genera $g_s \longrightarrow \infty$ such that:

1. X_s is *defined over* $\mathbf{F}_p$;
2. $g_{s+1}/g_s \longrightarrow 1$ (*density* of $(X_s)_s$);
3. $|X_s(\mathbf{F}_{p^{2t}})|/g_s \underset{s\to\infty}{\longrightarrow} p^t - 1$ (*Optimality over* $\mathbf{F}_{p^{2t}}$) ?

the Graal: Conjecture Y

Conjecture

Let p be a prime and $2t \geqslant 2$. Does there exist a family $(X_s)_{s\geqslant 1}$ of curves, with genera $g_s \longrightarrow \infty$ such that:

1. X_s is *defined over* $\mathbf{F}_p$;
2. $g_{s+1}/g_s \longrightarrow 1$ (*density* of $(X_s)_s$);
3. $|X_s(\mathbf{F}_{p^{2t}})|/g_s \underset{s\to\infty}{\longrightarrow} p^t - 1$ (*Optimality over* $\mathbf{F}_{p^{2t}}$) ?

- Classical modular curves $X_0(N)$? ⚠ $2t = 2$ only;
- Garcia–Stichtenoth's towers F_s ? ⚠ $g_{s+1}/g_s \sim p^{2t}$.
- Shimura curves $X_0(\mathcal{N})$? ⚠ $2t \geqslant 4 \Rightarrow$ defined over $\mathbf{F}_{p^t}$;

Hint: galoisian descent Theorem of $X_0(\mathfrak{N})_F$ over $\mathbf{Q}$

General criterion for descent over $\mathbf{Q}$

X an object over $F/\mathbf{Q}$ s.t.

1. X has *field of moduli* $\mathbf{Q}$;
2. X has *no automorphisms*.

Hypotheses here:

(i)-(iii) $\Gamma_0(\mathfrak{N})$ is a *Galois invariant* quaternionic group;

Hint: galoisian descent *Theorem of* $X_0(\mathfrak{N})_F$ *over* $\mathbb{Q}$

General criterion for descent over $\mathbb{Q}$

X an object over $F/\mathbb{Q}$ s.t.

1. X has *field of moduli* $\mathbf{Q}$;
2. X has *no automorphisms*.

Hypotheses here:

(i)-(iii) $\Gamma_0(\mathfrak{N})$ is a *Galois invariant* quaternionic group;

(iv) $\Gamma_0(1)$ is a triangle group;

Theorem B: Conjecture Y for p=3 and 2t=6

1. Hard work: *compute two towers* of Shimura curves over $\mathbf{F}_{3^6}$!

$$\ldots \xrightarrow{f_4} X_0(7^3) \xrightarrow{f_3} X_0(7^2) \xrightarrow{f_2} X_0(7^1) \xrightarrow{f_1} X_0(1)$$
$$\ldots \xrightarrow{g_4} X_0(8^3) \xrightarrow{g_3} X_0(8^2) \xrightarrow{g_2} X_0(8^1) \xrightarrow{g_1} X_0(1)$$

2. *Descend* everything over $\mathbf{F}_3$.

Theorem B: Conjecture Y for p=3 and 2t=6

1. Hard work: *compute two towers* of Shimura curves over $\mathbf{F}_{3^6}$!

$$\dots \xrightarrow{f_4} X_0(7^3) \xrightarrow{f_3} X_0(7^2) \xrightarrow{f_2} X_0(7^1) \xrightarrow{f_1} X_0(1)$$
$$\dots \xrightarrow{g_4} X_0(8^3) \xrightarrow{g_3} X_0(8^2) \xrightarrow{g_2} X_0(8^1) \xrightarrow{g_1} X_0(1)$$

2. *Descend* everything over $\mathbf{F}_3$.
3. Then for the density...

Elkies' Trick

$$
\begin{array}{ccccccccccc}
 & & & & & & & & & & \swarrow \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
X_0(7^4) & \longleftarrow & X_0(7^4 8^1) & \longleftarrow & X_0(7^4 8^2) & \longleftarrow & X_0(7^4 8^3) & \longleftarrow & X_0(7^4 8^4) & \leftarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
X_0(7^3) & \longleftarrow & X_0(7^3 8^1) & \longleftarrow & X_0(7^3 8^2) & \longleftarrow & X_0(7^3 8^3) & \longleftarrow & X_0(7^3 8^4) & \leftarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
X_0(7^2) & \longleftarrow & X_0(7^2 8^1) & \longleftarrow & X_0(7^2 8^2) & \longleftarrow & X_0(7^2 8^3) & \longleftarrow & X_0(7^2 8^4) & \leftarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
X_0(7^1) & \longleftarrow & X_0(7^1 8^1) & \longleftarrow & X_0(7^1 8^2) & \longleftarrow & X_0(7^1 8^3) & \longleftarrow & X_0(7^1 8^4) & \leftarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
X_0(1) & \longleftarrow & X_0(8^1) & \longleftarrow & X_0(8^2) & \longleftarrow & X_0(8^3) & \longleftarrow & X_0(8^4) & \leftarrow & \cdots
\end{array}
$$

The genus one Belyi map $X_0(7^2) \xrightarrow{f_2} X_0(7)$

Goal: j-invariant of $X_0(7^2)_{\mathbf{C}}$? Input: $\Gamma_0(7^2) \subset \mathrm{PSL}_2(\mathbf{R})$

Algorithm [Klug–Musty–Schiavone–Voight]

- Fundamental domain for $\Gamma_0(7^2)$.
- The differential form g on $X_0(7^2)_{\mathbf{C}}$:

$$g(w) = 1 - \frac{2}{3}\cdot w + \frac{2^3}{3^3}\cdot w^3 + \frac{2^7}{3^7\cdot 7}w^7 + \frac{2^7}{3^7\cdot 7}w^8 + \frac{2^9}{3^{10}\cdot 7^1}w^{10} - \frac{2^{13}\cdot 5}{3^{13}\cdot 7^2\cdot 13}w^{14} - \frac{2^{15}\cdot 5}{3^{15}\cdot 7^2\cdot 13}\cdot w^{15} + \frac{2^{15}}{3^{16}\cdot 7^2\cdot 13}w^{17} - \dots$$

- Periods of $g \to$ Periods lattice of $X_0(7^2)_{\mathbf{C}} \to j = -3375$.

The genus one Belyi map $X_0(7^2) \xrightarrow{f_2} X_0(7)$

Goal: canonical model of $X_0(7^2)$? Inputs:

- j-invariant: -3375;
- *Descends to an elliptic curve over* $\mathbf{Q}$ (specific Theorem);
- Conductor equals $7^{1 \text{ or } 2}$ (the Theory);
- Traces of Frobenius equals traces of quaternionic Hecke operators (the Theory).

Output: $X_0(7^2)_{\mathbf{Q}}$ is either 49.a2 or 49.a4 (LMFBD)

The genus one Belyi map $X_0(7^2) \xrightarrow{f_2} X_0(7)$

Goal: equation for f_2 ? Input: $\{49.a2$ or $49.a4\}$, ramification:

$$
\begin{array}{ccccccc}
X_0(7^2) & (3)^2 & & P_3 & P'_3 & & (3)^2 & (7) \\
\Big\downarrow{\scriptstyle f_2,\ 7} & & \searrow^{3^2} & \Big\downarrow{\scriptstyle 1} & \Big\downarrow{\scriptstyle 1} & \swarrow_{3^2} & & \Big\downarrow{\scriptstyle 7} \\
X_0(7) & & & Q_3 & Q'_3 & & & Q_7
\end{array}
$$

And monodromy: $[(1,6,4,2,7,5,3),(1,6,2)(4,5,7),(1,3,4)(2,7,6)]$
Method: [Sijsling & Voight]^2 for computation and descent.
Output : $X_0(7^2)_{\mathbf{Q}} = 49.a4$ and

$$f_2(x,y) = 2x + 5x^2 - 3x^3 + (-3 + 3x + x^2)y$$

Thank you for your attention

Not meant to be shown

$$X_0(8^3) = \quad X_0(8^2) \quad \times \quad X_0(8^2)$$

$$X_0(8^2) \xrightarrow{\omega_1 \circ f_2 \circ \omega_2} X_0(8^1) \xleftarrow{f_2} X_0(8^2)$$

$$X_0(8^2)_{\mathbf{F}_3} \quad : \quad y^2 = x^3 + x^2 + 2$$

$$X_0(8^1)_{\mathbf{F}_3} \quad : \quad \mathbf{P}^1_{\mathbf{F}_3}$$

$$f_2 : \quad (x, y) \longmapsto \frac{1+x^2+x^3+x^4+(x+2x^2)y}{2+x^2+x^3+x^4+x^2y}$$

$$\omega_2 : \quad X_0(8^2)_{\mathbf{F}_3} \ni P \longmapsto (1, 2, 1) - P$$

$$\omega_1 : \quad t \in \mathbf{P}^1_{\mathbf{F}_3} \ni t \longmapsto -t$$

of genus 7 and having 1760 points over $\mathbf{F}_{3^6}$, as predicted from traces of Hecke operators.

Not meant to be shown

$$
\begin{array}{c}
X_0(8^2) = \mathsf{Elliptic}_{/\mathbf{C}} \\
f_2 \Big\downarrow 8 \\
X_0(8^1) = \mathbf{P}^1_{\mathbf{C}} \\
f_1 \Big\downarrow 9 \\
X_0(1) = \mathbf{P}^1_{\mathbf{C}}
\end{array}
\qquad
\begin{array}{ccccccc}
(7) & & P_7 & & {P'}_7 & & (7) \\
& \overset{7}{\searrow} & \Big\downarrow 1 & & 1 \Big\downarrow & \overset{7}{\swarrow} & \\
(7) & & Q_7 & & Q'_7 & & (3)^3 \\
& \overset{7}{\searrow} & 1 \Big\downarrow & \overset{1}{\swarrow} & & & 3^3 \Big\downarrow \\
& & R_7 & & & & R_3
\end{array}
\qquad
\begin{array}{c}
(2)^4 \\
8 \Big\downarrow \\
Q_2\,,(2)^4 \\
1 \Big\downarrow 2^4 \\
R_2
\end{array}
$$