Calcul rapide d'isogénies en genre 1

Luca De Feo

INRIA Saclay, Projet TANC

21 Octobre 2010
Séminaire Crypto, Université de Caen, Paris

Plan

Isogénies entre courbes elliptiques

$$\mathcal{I} : E \to E'$$

Isogénie (separable) : morphisme rationnel (separable) non-constant préservant le point à l'infini.

Propriétés

- Noyau fini, surjective (dans $\bar{\mathbb{K}}$),
- définie par des fractions rationnelles avec un pôle à l'infini,
- $\#E(\mathbb{F}_{q^n}) = \#E'(\mathbb{F}_{q^n})$ pour tout n,
- Isogénie *duale* : $[m] = \mathcal{I} \circ \hat{\mathcal{I}}$.

Multiplication

$$\begin{aligned} [m] : E(\bar{\mathbb{K}}) &\to E(\bar{\mathbb{K}}) \\ P &\mapsto [m]P \end{aligned}$$

$\ker \mathcal{I} = E[m], \quad \deg \mathcal{I} = m^2.$

Isogénies entre courbes elliptiques

$$\mathcal{I} : E \to E'$$

Isogénie (separable) : morphisme rationnel (separable) non-constant préservant le point à l'infini.

Propriétés

- Noyau fini, surjective (dans $\bar{\mathbb{K}}$),
- définie par des fractions rationnelles avec un pôle à l'infini,
- $\#E(\mathbb{F}_{q^n}) = \#E'(\mathbb{F}_{q^n})$ pour tout n,
- Isogénie *duale* : $[m] = \mathcal{I} \circ \hat{\mathcal{I}}$.

Endomorphisme de Frobenius

$$\begin{aligned} \varphi : E(\bar{\mathbb{K}}) &\to E(\bar{\mathbb{K}}) \\ (X, Y) &\mapsto (X^q, Y^q) \end{aligned}$$

$\ker \varphi = \{\mathcal{O}\}, \quad \deg \mathcal{I} = q.$

Isogénies entre courbes elliptiques

$$\mathcal{I} : E \to E'$$

Isogénie (separable) : morphisme rationnel (separable) non-constant préservant le point à l'infini.

Propriétés

- Noyau fini, surjective (dans $\bar{\mathbb{K}}$),
- définie par des fractions rationnelles avec un pôle à l'infini,
- $\#E(\mathbb{F}_{q^n}) = \#E'(\mathbb{F}_{q^n})$ pour tout n,
- Isogénie *duale* : $[m] = \mathcal{I} \circ \hat{\mathcal{I}}$.

Isogénie separable, degré impair (modèle de Weierstrass simplifié)

$$\mathcal{I}(X, Y) = \left(\frac{g(X)}{h^2(X)}, cY \left(\frac{g(X)}{h^2(X)} \right)' \right)$$

$\ell = \deg \mathcal{I} = \# \ker \mathcal{I} = 2 \deg h + 1$ impair.

Schoof 1985

- $\#E(\mathbb{F}_q) = q + 1 - t$ avec t la *trace* du Frobenius : $\varphi^2 - [t] \circ \varphi + [q] = 0$;
- Calculer $t \bmod \ell$ pour les premiers $\ell < O(\log q)$;
- Équivalent à calculer l'action de φ sur $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$;
- **En pratique :** calculs modulo le *polynôme de division* (degré $\sim O(\ell^2)$).

Elkies (Elkies 1998 ; Schoof 1995)

- Par le théorème de l'isogénie duale $[\ell] = \mathcal{I} \circ \hat{\mathcal{I}}$;
- $E[\ell]$ contient le sous-groupe $\ker \mathcal{I} \cong \mathbb{Z}/\ell\mathbb{Z}$;
- Si $\mathcal{I}$ est définie sur $\mathbb{K}$:
  1. Trouver la courbe isogène $E/\ker \mathcal{I}$,
  2. calculer l'action de φ sur $\ker \mathcal{I}$,
  3. **En pratique :** calculs modulo le dénominateur de l'isogénie (degré $\sim O(\ell)$).
- Marche en moyenne pour la moitié des nombres premiers.

Atkin 1988...

Schoof 1985

- $\#E(\mathbb{F}_q) = q + 1 - t$ avec t la *trace* du Frobenius : $\varphi^2 - [t] \circ \varphi + [q] = 0$;
- Calculer $t \bmod \ell$ pour les premiers $\ell < O(\log q)$;
- Équivalent à calculer l'action de φ sur $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$;
- **En pratique :** calculs modulo le *polynôme de division* (degré $\sim O(\ell^2)$).

Elkies (Elkies 1998 ; Schoof 1995)

- Par le théorème de l'isogénie duale $[\ell] = \mathcal{I} \circ \hat{\mathcal{I}}$;
- $E[\ell]$ contient le sous-groupe $\ker \mathcal{I} \cong \mathbb{Z}/\ell\mathbb{Z}$;
- Si $\mathcal{I}$ est définie sur $\mathbb{K}$:
  1. Trouver la courbe isogène $E/\ker \mathcal{I}$,
  2. calculer l'action de φ sur $\ker \mathcal{I}$,
  3. **En pratique :** calculs modulo le dénominateur de l'isogénie (degré $\sim O(\ell)$).
- Marche en moyenne pour la moitié des nombres premiers.

Atkin 1988...

Cryptographie moderne

L'attaque de Gaudry, Hess et Smart 2002

- Calcule une isogénie $\mathcal{I} : E/\mathbb{F}_{q^d} \to H/\mathbb{F}_q$ par descente de Weil ;
- H hyperelliptique de genre $\sim d$: log discret sur H plus facile pour certains jeux de paramètres.

Le cryptosystème de Teske 2006

Pas toutes les courbes dans une classe d'isogénie sont vulnérables à GHS, cela permet d'obtenir un cryptosystème *à trappe* :

1. Sélectionner E GHS-vulnérable ;
2. Obtenir E' non-GHS-vulnérable par une marche aléatoire dans le graphe d'isogénies ;
3. Utiliser E' pour le matériel publique, donner E à une autorité de confiance.

Autres protocoles utilisant des isogénies

- Le protocole *à la Diffie-Hellman* de Rostovtsev et Stolbunov 2006,
- Fonctions de hachage : Charles, Lauter et Goren 2009.

Quelles entrées, quelles sorties ?

Entrées

1. Donnés E et un sous-groupe H de cardinal ℓ ;
2. Donnés E, ℓ ;
3. Donnés E, E' ;
4. Donnés E, E', ℓ ;

Sorties

A. Existence : dire s'il existe $\mathcal{I} : E \to E'$ (de noyau H, ou de degré ℓ) ;
B. Calculer : des expressions rationnelles en x et y pour $\mathcal{I}$.

- **1A, 2A :** Toujours vrai ;
- **3A :** $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$?

Plan

Formules de Vélu

Vélu 1971 (corps algébriquement clos)

Étant donné le noyau H, calcule $\mathcal{I} : E \to E/H$ donnée par

$$\mathcal{I}(\mathcal{O}_E) = \mathcal{I}(\mathcal{O}_{E/H}),$$

$$\mathcal{I}(P) = \left(x(P) + \sum_{Q \in H^*} x(P+Q) - x(Q), y(P) + \sum_{Q \in H^*} y(P+Q) - y(Q) \right).$$

Pour $p \geqslant 3$, étant donné $h(x)$ s'annulant sur H

$$y^2 = f(x) = x^3 + a_2 x^2 + a_4 x + a_6, \quad t = \sum_{Q \in H^*} f'(Q), \quad u = \sum_{Q \in H^*} 2f(Q), \quad w = u + \sum_{Q \in H^*} x(Q) f'(Q),$$

$$\mathcal{I}(x,y) = \left(\frac{g(x)}{h(x)}, y \left(\frac{g(x)}{h(x)} \right)' \right) \quad \text{avec} \quad \frac{g(x)}{h(x)} = x + t\frac{h'(x)}{h(x)} - u \left(\frac{h'(x)}{h(x)} \right)'$$

$$E/H : y^2 = x^3 + a_2 x^2 + (a_4 - 5t)x + a_6 - 4a_2 t - 7w$$

Polynôme modulaire

$\Phi_\ell(X, Y)$, le polynôme minimal sur $\mathbb{C}$ de la fonction modulaire $j(\ell\tau)$

Propriétés

- Les racines de $\Phi_\ell(X, j(E))$ sont les j-invariants des courbes ℓ-isogènes à E ;
- Symétrique en X et Y, degré $\ell + 1$;
- Coefficients entiers de taille $O(\ell)$.

En pratique

- On utilise plutôt d'autres invariants modulaires, mais la théorie ne change pas ;
- Plusieurs tables de polynômes modulaires précalculés (Enge-Morain, Magma, ...) ;
- Calcul en $\tilde{O}(\ell^3)$ par Broker, Lauter et Sutherland 2010 ;
- et aussi : calcul de $\Phi_\ell \bmod m$ en $\tilde{O}(\ell^2 \log m)$.

Bostan, Morain, Salvy et Schost 2008

Donnés E, E', ℓ, calculer $\mathcal{I} : E \to E'$

Par les formules de Vélu : $\mathcal{I}(x,y) = \left(\frac{g(x)}{h(x)}, cy\left(\frac{g(x)}{h(x)}\right)'\right)$, d'où

$$c^2(x^3+ax+b)\left(\frac{g(x)}{h(x)}\right)'^2 = \left(\frac{g(x)}{h(x)}\right)^3 + a'\frac{g(x)}{h(x)} + b'$$

Algorithme BMSS

1. Changement de variables $S(x) = \sqrt{\frac{h(1/x^2)}{g(1/x^2)}} \quad \Leftrightarrow \quad \frac{g(x)}{h(x)} = \frac{1}{S(1/\sqrt{x})^2}$;
2. Solution série de l'équa diff $c^2(bx^6+ax^4+1)S'^2 = 1 + a'S^4 + b'S^6$;
3. Inverser le changement de variables, reconstruire une fraction rationnelle.

Bostan, Morain, Salvy et Schost 2008

Donnés E, E', ℓ, calculer $\mathcal{I} : E \to E'$

Par les formules de Vélu : $\mathcal{I}(x,y) = \left(\frac{g(x)}{h(x)}, cy\left(\frac{g(x)}{h(x)}\right)'\right)$, d'où

$$c^2(x^3+ax+b)\left(\frac{g(x)}{h(x)}\right)'^2 = \left(\frac{g(x)}{h(x)}\right)^3 + a'\frac{g(x)}{h(x)} + b'$$

Algorithme BMSS

1. Changement de variables $S(x) = \sqrt{\frac{h(1/x^2)}{g(1/x^2)}} \quad \Leftrightarrow \quad \frac{g(x)}{h(x)} = \frac{1}{S(1/\sqrt{x})^2}$;
2. Solution série de l'équa diff $c^2(bx^6+ax^4+1)S'^2 = 1 + a'S^4 + b'S^6$;
3. Inverser le changement de variables, reconstruire une fraction rationnelle.

Quelles entrées, quelles sorties ?

Entrées

1. Donnés E et un sous-groupe H de cardinal ℓ ;
2. Donnés E, ℓ ;
3. Donnés E, E' ;
4. Donnés E, E', ℓ ;

Sorties

A. Existence : dire s'il existe $\mathcal{I} : E \to E'$ (de noyau H, ou de degré ℓ) ;
B. Calculer : des expressions rationnelles en x et y pour $\mathcal{I}$.

- **1B :** Formules de Vélu ;
- **4A :** $\Phi_\ell(j(E), j(E')) = 0$?
- **4B** $\Rightarrow$ **2B :** Factoriser $\Phi_\ell(X, j(E))$;
- **4B :** BMSS, si possible...
- **3B :** ? ? ?

SEA

Pour tout $\ell \sim \log q$ premier d'Elkies

1. Trouver une racine j' de $\Phi_\ell(X, j(E))$;
2. En déduire une courbe

$$E' : y^2 = x^3 + ax + b \quad \text{avec} \quad j(E') = j',$$

   ℓ-isogène à E ;
3. Utiliser BMSS pour calculer $\mathcal{I} : E \to E'$;
4. En déduire $t \bmod \ell$.

SEA

Pour tout $\ell \sim \log q$ premier d'Elkies

1. Trouver une racine j' de $\Phi_\ell(X, j(E))$;
2. En déduire une courbe

$$E' : y^2 = x^3 + ax + b \quad \text{avec} \quad j(E') = j',$$

   ℓ-isogène à E ;
3. Utiliser BMSS pour calculer $\mathcal{I} : E \to E'$;
4. En déduire $t \bmod \ell$.

Isogénies canoniques

En général pour le modèle de Weierstrass $\mathcal{I}(x,y) = \left(\frac{g(x)}{h(x)}, cy\left(\frac{g(x)}{h(x)}\right)'\right)$,

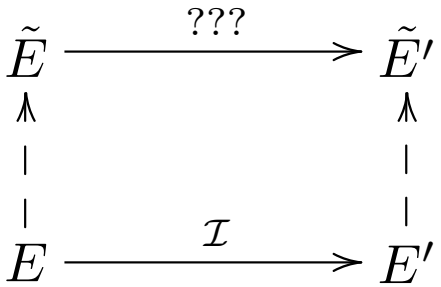
- Quand $c = 1$ on dit que le modèles de E et E' sont *canoniques* ou *strictes* ou *normalisés* ;
- Dans le cadre de SEA, Elkies 1998 obtient un modèle normalisé $E'' \cong E'$ en évaluant les dérivées partielles de Φ_ℓ.

- **1B :** Formules de Vélu ..... $O(\ell)$;
- **4A :** $\Phi_\ell(j(E), j(E')) = 0$? ..... $\tilde{O}(\ell^2)$;
- **2B :** Factoriser $\Phi_\ell(X, j(E))$ + Elkies 1998 + BMSS ..... $\tilde{O}(\ell^2)$;
- **4B :** BMSS, seulement dans le cas *canonique* ..... $\tilde{O}(\ell)$;
- **2B** $\Rightarrow$ **4B :** Elkies 1998 + BMSS + isomorphisme ..... $\tilde{O}(\ell^2)$;
- **3B :** ? ? ?

Plan

Lercier et Sirvent 2008

Idée : Lifter dans les p-adiques
Problème : Comment maintenir des modèles normalisés ?



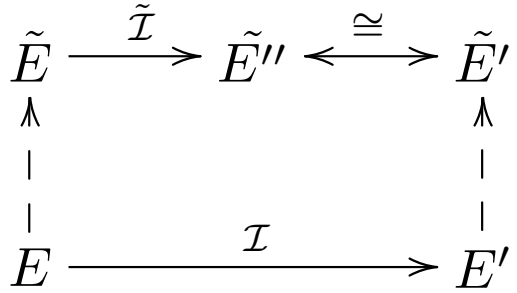
Lercier et Sirvent 2008

Idée : Lifter dans les p-adiques
Problème : Comment maintenir des modèles normalisés ?

Algorithme

1. Lifter j et j' en maintenant $\Phi_\ell(\tilde{j}, \tilde{j}') = 0$;
2. Lifter E ;
3. Calculer un modèle ℓ-normalisé pour $\tilde{j}'$ par Elkies 1998 ;
4. Appliquer BMSS dans $\mathbb{Q}_q$.

Précision p-adique requise $O(\log^2 \ell)$, complexité totale $\tilde{O}(\ell^2)$,
même dans le cas *canonique* !



SEA revisité

Pour tout $\ell \sim \log q$ premier d'Elkies

1. Lifter E dans $\mathbb{Q}_q$;
2. Trouver une racine $\tilde{j}'$ dans $\mathbb{Q}_q$ de $\Phi_\ell(X, j(\tilde{E}))$;
3. Par Elkies 1998, obtenir une courbe

$$\tilde{E}' : y^2 = x^3 + ax + b \quad \text{avec} \quad j(\tilde{E}') = \tilde{j}',$$

   ℓ-isogène à $\tilde{E}$;
4. Utiliser BMSS dans $\mathbb{Q}_q$ pour calculer $\tilde{\mathcal{I}} : \tilde{E} \to \tilde{E}'$;
5. Réduire $\tilde{I}$ dans $\mathbb{F}_q$;
6. En déduire $t \bmod \ell$.

Les algorithmes de Couveignes

Idée : Envoyer $E[p^k]$ sur $E'[p^k]$

Couveignes 1994

Couveignes 1996

- Calculer itérativement les extensions $\mathbb{U}_i/\mathbb{F}_q$ t.q. $E[p^i]$ est défini dans $\mathbb{U}_i$;
- Sélectionner un k *assez grand* $(k \sim \log_p 4\ell)$;
- Calculer P, générateur de $E[p^k]$;
- Calculer P', générateur de $E'[p^k]$;
- Calculer le polynôme T s'annulant sur $E[p^k]$;
- Interpoler $A : x(P) \mapsto x(P')$;
- Reconstruire une fraction rationnelle $\frac{g}{h} \equiv A \bmod T$;
- Si $\frac{g}{h}$ est une isogénie, fini ; sinon choisir un autre P'.

Les algorithmes de Couveignes

Idée : Envoyer $E[p^k]$ sur $E'[p^k]$

Couveignes 1994

- Passer dans le groupe formel $\mathcal{E}$ de E : un *point formel* est une série en un paramètre formel τ ;
- Fixer une précision *assez grande* pour $\mathbb{F}_q[[\tau]]$ ($\sim \log_p 4\ell$) ;
- Calculer un morphisme $\mathcal{U}(\tau) : \mathcal{E} \to \mathcal{E}'$;
- Reconstruire une fraction rationnelle $\frac{g(X)}{h(X)} = \frac{1}{\mathcal{U}(1/X)}$;
- Si $\frac{g}{h}$ est une isogénie, fini ; sinon choisir un autre $\mathcal{U}$.

Couveignes 1996

- Calculer itérativement les extensions $\mathbb{U}_i/\mathbb{F}_q$ t.q. $E[p^i]$ est défini dans $\mathbb{U}_i$;
- Sélectionner un k *assez grand* ($k \sim \log_p 4\ell$) ;
- Calculer P, générateur de $E[p^k]$;
- Calculer P', générateur de $E'[p^k]$;
- Calculer le polynôme T s'annulant sur $E[p^k]$;
- Interpoler $A : x(P) \mapsto x(P')$;
- Reconstruire une fraction rationnelle $\frac{g}{h} \equiv A \bmod T$;
- Si $\frac{g}{h}$ est une isogénie, fini ; sinon choisir un autre P'.

Les algorithmes de Couveignes

Idée : Envoyer $E[p^k]$ sur $E'[p^k]$

Couveignes 1994

- Passer dans le groupe formel $\mathcal{E}$ de E : un *point formel* est une série en un paramètre formel τ ;
- Fixer une précision *assez grande* pour $\mathbb{F}_q[[\tau]]$ ($\sim \log_p 4\ell$) ;
- Calculer un morphisme $\mathcal{U}(\tau) : \mathcal{E} \to \mathcal{E}'$;
- Reconstruire une fraction rationnelle $\frac{g(X)}{h(X)} = \frac{1}{\mathcal{U}(1/X)}$;
- Si $\frac{g}{h}$ est une isogénie, fini ; sinon choisir un autre $\mathcal{U}$.
- $\mathcal{U}$ est uniquement déterminé par son action sur $\mathcal{E}[p^k]$ pour tout k.

Couveignes 1996

- Calculer itérativement les extensions $\mathbb{U}_i/\mathbb{F}_q$ t.q. $E[p^i]$ est défini dans $\mathbb{U}_i$;
- Sélectionner un k *assez grand* ($k \sim \log_p 4\ell$) ;
- Calculer P, générateur de $E[p^k]$;
- Calculer P', générateur de $E'[p^k]$;
- Calculer le polynôme T s'annulant sur $E[p^k]$;
- Interpoler $A : x(P) \mapsto x(P')$;
- Reconstruire une fraction rationnelle $\frac{g}{h} \equiv A \bmod T$;
- Si $\frac{g}{h}$ est une isogénie, fini ; sinon choisir un autre P'.

Comment reconnaître une isogénie ?

- **Degré** : $\frac{g}{h}$ avec $\deg g = \ell$, $\deg h = \ell - 1$; $O(1)$
- **Facteur carré :** $h = \prod_{Q \in H^*}(X - x(Q)) = f^2$ si ℓ impair ; $\tilde{O}(\ell)$
- **Action de groupe :** Tester avec des points au hasard ; $O(\ell)$
- **Facteur du polynôme de ℓ-division :** Calculer $\phi_\ell \bmod h$. $\tilde{O}(\ell)$

Comment reconnaître une isogénie ?

$$AU_i + TV_i = R_i \qquad \Leftrightarrow \qquad A \equiv \frac{R_i}{U_i} \bmod T$$

$$\ell = 11$$

Comment reconnaître une isogénie ?

$$AU_i + TV_i = R_i \qquad \Leftrightarrow \qquad A \equiv \frac{R_i}{U_i} \bmod T$$

$$\ell = 11$$

$$\deg R_i \qquad \Big| \qquad \deg U_i$$

Comment reconnaître une isogénie ?

$$AU_i + TV_i = R_i \qquad \Leftrightarrow \qquad A \equiv \frac{R_i}{U_i} \bmod T$$

$$\ell = 11$$

$\deg R_i$	$\deg U_i$
$31415926535897932384626\,43$	0

Comment reconnaître une isogénie ?

$$AU_i + TV_i = R_i \qquad \Leftrightarrow \qquad A \equiv \frac{R_i}{U_i} \bmod T$$

$$\ell = 11$$

$\deg R_i$	$\deg U_i$
$31415926535897932384626\,43$	0
$31415926535897932384626\,42$	1

Comment reconnaître une isogénie ?

$$AU_i + TV_i = R_i \qquad \Leftrightarrow \qquad A \equiv \frac{R_i}{U_i} \bmod T$$

$$\ell = 11$$

$\deg R_i$	$\deg U_i$
31415926535897932384626643	0
31415926535897932384626642	1
31415926535897932384626641	2

Comment reconnaître une isogénie ?

$$AU_i + TV_i = R_i \qquad \Leftrightarrow \qquad A \equiv \frac{R_i}{U_i} \bmod T$$

$$\ell = 11$$

$\deg R_i$	$\deg U_i$
$314159265358979323846264 3$	0
$314159265358979323846264 2$	1
$314159265358979323846264 1$	2
$\vdots$	$\vdots$
$314159265358979323846263 4$	9

Comment reconnaître une isogénie ?

$$AU_i + TV_i = R_i \qquad \Leftrightarrow \qquad A \equiv \frac{R_i}{U_i} \bmod T$$

$$\ell = 11$$

$\deg R_i$	$\deg U_i$
31415926535897932384626643	0
31415926535897932384626642	1
31415926535897932384626641	2
$\vdots$	$\vdots$
31415926535897932384626634	9

Comment reconnaître une isogénie ?

$$AU_i + TV_i = R_i \qquad \Leftrightarrow \qquad A \equiv \frac{R_i}{U_i} \bmod T$$

$$\ell = 11$$

$\deg R_i$	$\deg U_i$
314159265358979323846264 3	0
314159265358979323846264 2	1
314159265358979323846264 1	2
$\vdots$	$\vdots$
314159265358979323846263 4	9
11	10

Comment reconnaître une isogénie ?

$$AU_i + TV_i = R_i \qquad \Leftrightarrow \qquad A \equiv \frac{R_i}{U_i} \bmod T$$

$$\ell = 11$$

$\deg R_i$	$\deg U_i$
$3141592653589793238462643$	0
$3141592653589793238462642$	1
$3141592653589793238462641$	2
$\vdots$	$\vdots$
$3141592653589793238462634$	9
11	10
10	$3141592653589793238462633$
$\vdots$	$\vdots$

Isogénies de degré inconnu

- Ce *pattern* est extrêmement rare.
- Ceci est la seule partie des algorithmes de Couveignes qui dépend de ℓ.

Isogénies de degré inconnu

- Ce *pattern* est extrêmement rare.
- Ceci est la seule partie des algorithmes de Couveignes qui dépend de ℓ.
- En fait, cela ne dépend pas vraiment de ℓ, mais juste de la présence d'un *saut*.
- Si ℓ n'est pas connu à l'avance, il suffit d'attendre un *saut*.
- Ainsi, toutes les isogénies de degré $\ll p^k$ peuvent être obtenues avec une seule exécution des algorithmes de Couveignes.

Isogénies de degré inconnu

- Ce *pattern* est extrêmement rare.
- Ceci est la seule partie des algorithmes de Couveignes qui dépend de ℓ.
- En fait, cela ne dépend pas vraiment de ℓ, mais juste de la présence d'un *saut*.
- Si ℓ n'est pas connu à l'avance, il suffit d'attendre un *saut*.
- Ainsi, toutes les isogénies de degré $\ll p^k$ peuvent être obtenues avec une seule exécution des algorithmes de Couveignes.
- Mais pourquoi ? Et ça sert à quoi ?

Plan

Quelques temps d'exécution

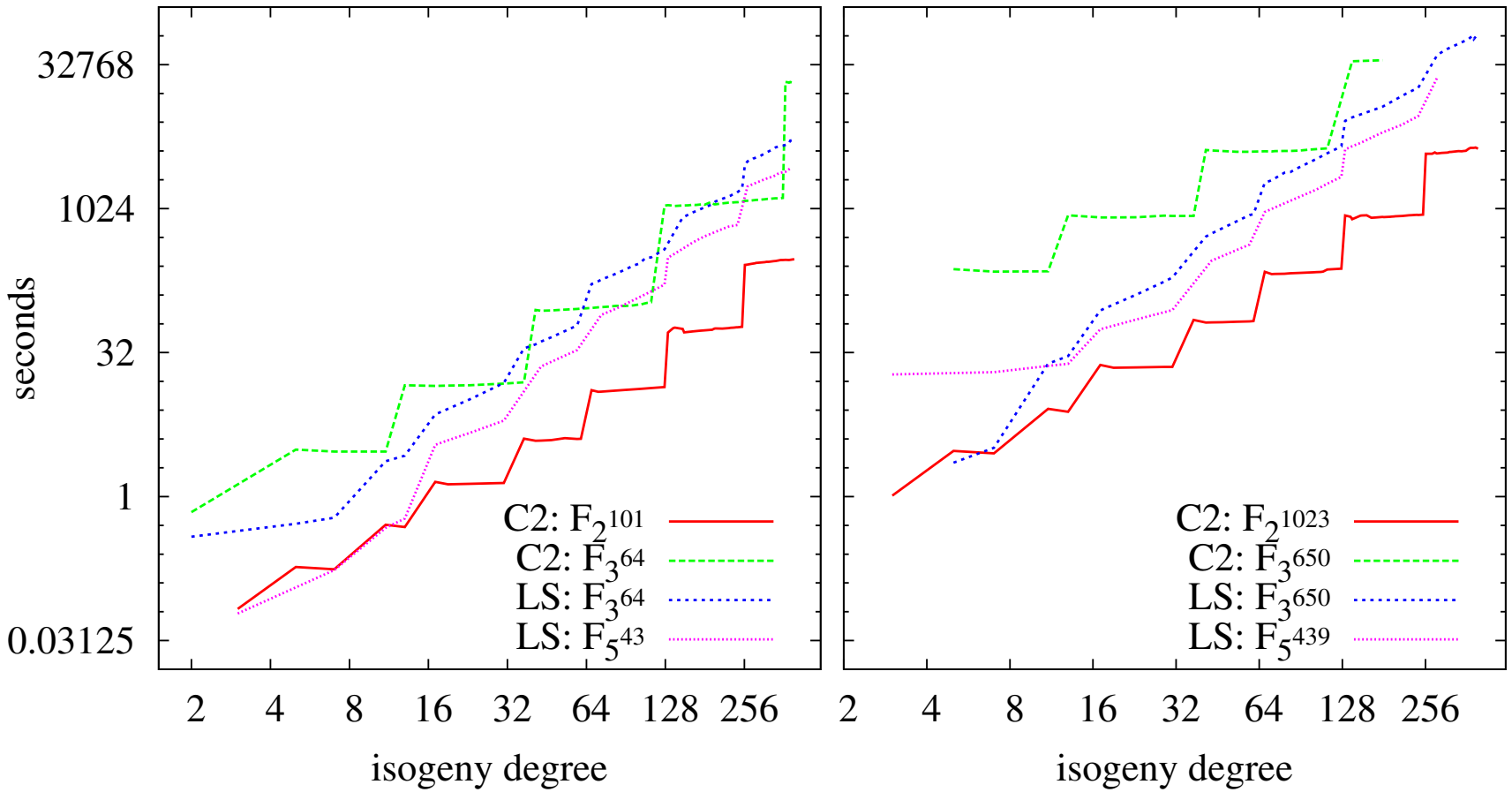


FIGURE: Comparaison des temps d'exécution de COUVEIGNES 1996 (C2, seul le temps moyen est dessiné) et LERCIER et SIRVENT 2008 (LS) sur plusieurs courbes et corps de base. Processeur Intel Xeon E5520 (Nehalem) @2.26GHz. Échelle logarithmique.

Marathon d'implantations

- `FAAST`, pour l'arithmétique dans les tours d'Artin-Schreier, implantée en `C++` et distribuée sous GPL : `http://www.lix.polytechnique.fr/~defeo/FAAST`
- Implantation de Couveignes 1996 basée sur FAAST, pas encore distribuée.
- Lercier-Sirvent en Magma, en attendant une version en `C++`.
- Lercier ($p = 2$) en `C++` par F. Morain.
- Librairie de calcul d'isogénies en développement, effort joint avec F. Morain, É. Schost.
- Portage pour SAGE. . .un jour ?

Perspectives

En quête de la complexité quasi-linéaire

- Weierstrass a un défaut de canonicité : autres paramétrisations ?
- Comment obtenir de l'information *locale* sur le comportement de l'isogénie ? (par exemple, son action sur $E[p]$)

Isogénies de degré inconnu

- Testé deux courbes sur $\mathbb{F}_{2^{161}}$ isogènes de degré inconnu, prises de Teske 2006 ;
- Certifié en 258 heures-cpu qu'il n'y a aucune isogénie de degré $2^c\ell$ pour c quelconque et $\ell < 2^{11}$;
- Certifié en 1195 heures-cpu qu'il n'y a aucune isogénie de degré inférieur à 2^{12}.
- Les courbes ont une isogénie de degré (très friable) $\sim 2^{1050}$. Prouver qu'aucune isogénie de degré plus petit existe est actuellement hors porté.

Z'en voulez plus ?

Fast Algorithms for Towers of Finite Fields and Isogenies

13 décembre, École Polytechnique
heure et amphi à préciser

References I

Couveignes, Jean-Marc (1994).
"Quelques calculs en théorie des nombres".
Thèse de doct. Université de Bordeaux.

Schoof, René (1985).
"Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p".
Dans : *Mathematics of Computation* 44.170 ,
P. 483–494.
URL : http://dx.doi.org/10.2307/2007968.

References II

Elkies, Noam D. (1998).
"Elliptic and modular curves over finite fields and related computational issues".
Dans : *Computational perspectives on number theory (Chicago, IL, 1995)*.
T. 7.
Studies in Advanced Mathematics.
Providence, RI : AMS International Press,
P. 21–76.
URL : http://www.ams.org/mathscinet-getitem?mr=1486831.

Schoof, René (1995).
"Counting points on elliptic curves over finite fields".
Dans : *Journal de Théorie des Nombres de Bordeaux* 7.1 ,
P. 219–254.
URL : http://www.ams.org/mathscinet-getitem?mr=1413578.

Atkin, A. O. L. (1988).
"The number of points on an elliptic curve modulo a prime".
manuscript, Chicago IL.

References III

Gaudry, Pierrick, Florian Hess et Niegel Smart (2002).
"Constructive and destructive facets of Weil descent on elliptic curves".
Dans : *Journal of Cryptology* 15.1 ,
P. 19–46–46.
URL : http://dx.doi.org/10.1007/s00145-001-0011-x.

Teske, Edlyn (2006).
"An Elliptic Curve Trapdoor System".
Dans : *Journal of Cryptology* 19.1 ,
P. 115–133.
URL : http://dx.doi.org/10.1007/s00145-004-0328-3.

Rostovtsev, Alexander et Anton Stolbunov (2006).
Public-key Cryptosystem Based On Isogenies .
URL : http://eprint.iacr.org/2006/145.

References IV

Charles, Denis, Kristin Lauter et Eyal Goren (2009).
"Cryptographic Hash Functions from Expander Graphs".
Dans : *Journal of Cryptology* 22.1 ,
P. 93–113.
URL : http://dx.doi.org/10.1007/s00145-007-9002-x.

Vélu, Jean (1971).
"Isogénies entre courbes elliptiques".
Dans : *Comptes Rendus de l'Académie des Sciences de Paris* 273 ,
P. 238–241.

Broker, Reinier, Kristin Lauter et Andrew V. Sutherland (2010).
Modular polynomials via isogeny volcanoes .
URL : http://arxiv.org/abs/1001.0402.

References V

Bostan, Alin, François Morain, Bruno Salvy et Éric Schost (2008).
"Fast algorithms for computing isogenies between elliptic curves".
Dans : *Mathematics of Computation* 77 ,
P. 1755–1778.
URL : http://dx.doi.org/10.1090/S0025-5718-08-02066-8.

Lercier, Reynald et Thomas Sirvent (2008).
"On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field".
Dans : *Journal de théorie des nombres de Bordeaux* 20.3 ,
P. 783–797.
URL :
http://perso.univ-rennes1.fr/reynald.lercier/file/LS08.pdf.

References VI

Couveignes, Jean-Marc (1996).
"Computing l-Isogenies Using the p-Torsion".
Dans : *ANTS-II : Proceedings of the Second International Symposium on Algorithmic Number Theory* .
London, UK : Springer-Verlag,
P. 59–65.
URL : http://portal.acm.org/citation.cfm?id=749581.