Quelles courbes elliptiques pour la cryptographie ?

Christophe Ritzenthaler

19 mars 2008

C. Ritzenthaler, C.N.R.S. Institut de Mathématiques de Luminy
Luminy Case 930, F13288 Marseille CEDEX 9
e-mail : ritzenth@iml.univ-mrs.fr
web : http ://iml.univ-mrs.fr/∼ritzenth/

Des primitives cryptographiques aux applications

Primitives (AES, RSA, DLP)

fonctions crypto de bases
sécurité élémentaire

Des primitives cryptographiques aux applications

Primitives (AES, RSA, DLP)	fonctions crypto de bases sécurité élémentaire
↓	
Algorithmes (CBC-AES, RSA-OAEP)	sécurité renforcée model théorique pour l'attaquant

Des primitives cryptographiques aux applications

Primitives (AES, RSA, DLP)	fonctions crypto de bases sécurité élémentaire
↓	
Algorithmes (CBC-AES, RSA-OAEP)	sécurité renforcée model théorique pour l'attaquant
↓	
Protocoles (SSH, SSL)	attaques sur le protocole

Des primitives cryptographiques aux applications

Primitives (AES, RSA, DLP)	fonctions crypto de bases sécurité élémentaire
↓	
Algorithmes (CBC-AES, RSA-OAEP)	sécurité renforcée model théorique pour l'attaquant
↓	
Protocoles (SSH, SSL)	attaques sur le protocole
↓	
Implantation (openSSH, openSSL)	

Des primitives cryptographiques aux applications

Primitives (AES, RSA, DLP)	fonctions crypto de bases sécurité élémentaire
$\downarrow$	
Algorithmes (CBC-AES, RSA-OAEP)	sécurité renforcée model théorique pour l'attaquant
$\downarrow$	
Protocoles (SSH, SSL)	attaques sur le protocole
$\downarrow$	
Implantation (openSSH, openSSL)	
$\downarrow$	
Produit (https)	applications pour les usagers

Institut de Mathématiques de Luminy

Des primitives cryptographiques aux applications

Primitives (AES, RSA, DLP)	fonctions crypto de bases sécurité élémentaire
↓	
Algorithmes (CBC-AES, RSA-OAEP)	sécurité renforcée model théorique pour l'attaquant
↓	
Protocoles (SSH, SSL)	attaques sur le protocole
↓	
Implantation (openSSH, openSSL)	
↓	
Produit (https)	applications pour les usagers
↓	
Gestion humaine	changer 'password' admin.

Soit $(G =< g >, +)$ un groupe cyclique d'ordre N.

Echange de clés : Diffie-Hellman

Soit $(G =< g >, +)$ un groupe cyclique d'ordre N.

Alice		Bob
k_A aléatoire		k_B aléatoire
$h_A = k_A g$		$h_B = k_B g$

Echange de clés : Diffie-Hellman

Soit $(G =< g >, +)$ un groupe cyclique d'ordre N.

Alice		Bob
k_A aléatoire		k_B aléatoire
$h_A = k_A g$		$h_B = k_B g$
	$\xrightarrow{h_A}$	
	$\xleftarrow{h_B}$	

Echange de clés : Diffie-Hellman

Soit $(G =< g >, +)$ un groupe cyclique d'ordre N.

Alice		Bob
k_A aléatoire		k_B aléatoire
$h_A = k_A g$		$h_B = k_B g$
	$\xrightarrow{h_A}$	
	$\xleftarrow{h_B}$	
secret $= k_A h_B$		secret $= k_B h_A$

Echange de clés : Diffie-Hellman

Soit $(G =< g >, +)$ un groupe cyclique d'ordre N.

Alice		Bob
k_A aléatoire		k_B aléatoire
$h_A = k_A g$		$h_B = k_B g$
	$\xrightarrow{h_A}$	
	$\xleftarrow{h_B}$	
secret $= k_A h_B$		secret $= k_B h_A$

$\boxed{k_A k_B g \text{ est le secret commun}}$

Soit $(G =< g >, +)$ un groupe cyclique d'ordre N.

Alice		Bob
k_A aléatoire		k_B aléatoire
$h_A = k_A g$		$h_B = k_B g$
	$\xrightarrow{h_A}$	
	$\xleftarrow{h_B}$	
secret $= k_A h_B$		secret $= k_B h_A$

$\boxed{k_A k_B g \text{ est le secret commun}}$

A priori, la difficulté pour l'attaquant est de calculer $k_A k_B g$ connaissant $k_A g$ et $k_B g$ (DH calculatoire). C'est possible s'il sait résoudre le ...

Problème du logarithme discret (DLP)

Définition : Etant donné $(G =< g >, +)$ un groupe cyclique d'ordre N et $h \in G$ le DLP est de trouver un entier λ tel que

$$h = \lambda g.$$

Institut de Mathématiques de Luminy

Problème du logarithme discret (DLP)

Définition : Etant donné $(G =< g >, +)$ un groupe cyclique d'ordre N et $h \in G$ le DLP est de trouver un entier λ tel que

$$h = \lambda g.$$

Est ce équivalent au problème de DH calculatoire ?

Problème du logarithme discret (DLP)

Définition : Etant donné ($G =< g >, +$) un groupe cyclique d'ordre N et $h \in G$ le DLP est de trouver un entier λ tel que

$$h = \lambda g.$$

Est ce équivalent au problème de DH calculatoire ?

Oui si $\#G$ n'est pas divisible par le carré d'un grand nombre premier (Maurer-Wolf 1999).

Quelles sont les contraintes générales ?

- Efficacité : les éléments peuvent être stockés de manière compacte ($\log_2 N + \mathcal{O}(1)$ bits).

Quelles sont les contraintes générales ?

- Efficacité : les éléments peuvent être stockés de manière compacte ($\log_2 N + \mathcal{O}(1)$ bits).
- La loi de groupe est rapide : $\mathcal{O}(\log N)^{\mu}$ avec $\mu \geq 1$ petit.

Quelles sont les contraintes générales ?

- Efficacité : les éléments peuvent être stockés de manière compacte ($\log_2 N + \mathcal{O}(1)$ bits).
- La loi de groupe est rapide : $\mathcal{O}(\log N)^{\mu}$ avec $\mu \geq 1$ petit.
- Résistance aux attaques basiques
  - Paradoxe des anniversaires $\rightsquigarrow$ ρ-Pollard en $\mathcal{O}(\sqrt{N})$ heuristique (Kim-Montenegro-Tetali (Arxiv08) : collisions en $\mathcal{O}(\sqrt{N \log N \log \log N})$).

Quelles sont les contraintes générales ?

- Efficacité : les éléments peuvent être stockés de manière compacte ($\log_2 N + \mathcal{O}(1)$ bits).
- La loi de groupe est rapide : $\mathcal{O}(\log N)^{\mu}$ avec $\mu \geq 1$ petit.
- Résistance aux attaques basiques
  - Paradoxe des anniversaires $\rightsquigarrow$ ρ-Pollard en $\mathcal{O}(\sqrt{N})$ heuristique (Kim-Montenegro-Tetali (Arxiv08) : collisions en $\mathcal{O}(\sqrt{N \log N \log\log N})$).
  - Pohlig-Hellman : le temps de calcul est dominé par le DLP dans un groupe d'ordre le plus grand facteur premier de N $\rightsquigarrow$ N possède un grand facteur premier.

Institut de Mathématiques de Luminy

Quelles sont les contraintes générales ?

- Efficacité : les éléments peuvent être stockés de manière compacte ($\log_2 N + \mathcal{O}(1)$ bits).
- La loi de groupe est rapide : $\mathcal{O}(\log N)^\mu$ avec $\mu \geq 1$ petit.
- Résistance aux attaques basiques
  - Paradoxe des anniversaires $\rightsquigarrow$ ρ-Pollard en $\mathcal{O}(\sqrt{N})$ heuristique (Kim-Montenegro-Tetali (Arxiv08) : collisions en $\mathcal{O}(\sqrt{N \log N \log\log N})$).
  - Pohlig-Hellman : le temps de calcul est dominé par le DLP dans un groupe d'ordre le plus grand facteur premier de N $\rightsquigarrow$ N possède un grand facteur premier.
  - Résultat de Shoup : pour les groupes "génériques" $\mathcal{O}(\sqrt{N})$ au mieux.

- $(\mathbb{Z}/p\mathbb{Z})^*$ et plus généralement les groupes multiplicatifs des corps finis $\mathbb{F}_{p^n}$. Très efficaces mais il existe une attaque sous-exponentielle :
    - n petit : NFS en $L_{p^n}(1/3, (64/9)^{1/3})$.
    - p petit : FFS en $L_{p^n}(1/3, (32/9)^{1/3})$.

Les groupes candidats

- $(\mathbb{Z}/p\mathbb{Z})^*$ et plus généralement les groupes multiplicatifs des corps finis $\mathbb{F}_{p^n}$. Très efficaces mais il existe une attaque sous-exponentielle :
  - n petit : NFS en $L_{p^n}(1/3, (64/9)^{1/3})$.
  - p petit : FFS en $L_{p^n}(1/3, (32/9)^{1/3})$.

  Lercier : DLP sur $\mathbb{F}_p^*$ avec un p de 530 bits.
- groupe des classes $Cl(O_K)$ avec $K = \mathbb{Q}(\sqrt{-d})$ $(d > 1)$: attaque sous-exponentielle.

Les groupes candidats

- $(\mathbb{Z}/p\mathbb{Z})^*$ et plus généralement les groupes multiplicatifs des corps finis $\mathbb{F}_{p^n}$. Très efficaces mais il existe une attaque sous-exponentielle :
  - n petit : NFS en $L_{p^n}(1/3, (64/9)^{1/3})$.
  - p petit : FFS en $L_{p^n}(1/3, (32/9)^{1/3})$.

  Lercier : DLP sur $\mathbb{F}_p^*$ avec un p de 530 bits.
- groupe des classes $Cl(O_K)$ avec $K = \mathbb{Q}(\sqrt{-d})$ $(d > 1)$: attaque sous-exponentielle.
- Les points rationnels sur les jacobiennes de courbes de genre $g \geq 1$ sur $\mathbb{F}_q$.

Le calcul de l'index

Initié en 1994 par Adleman-DeMarrais-Huang.
Asymptotiques (Enge-Gaudry) : si $g/\log q \to \infty$ alors $L_{q^g}(\sqrt{2})$.

	$g=1$	$g=2$	$g=3$	$g=4$
Générique en $\sqrt{q^g}$	$q^{1/2}$	q	$q^{3/2}$	q^2
Calcul de l'index (2000)	-	-	q^2	q^2
Base réduite (2000)	-	-	$q^{3/2}$	$q^{8/5}$
Single large prime (2003)	-	-	$q^{10/7}$	$q^{14/9}$
Double large prime (2005)	-	-	$q^{4/3}$	$q^{3/2}$
Bas degré (2006)	-	-	q	

Initié en 1994 par Adleman-DeMarrais-Huang.
Asymptotiques (Enge-Gaudry) : si $g/\log q \to \infty$ alors $L_{q^g}(\sqrt{2})$.

	$g=1$	$g=2$	$g=3$	$g=4$
Générique en $\sqrt{q^g}$	$q^{1/2}$	q	$q^{3/2}$	q^2
Calcul de l'index (2000)	-	-	q^2	q^2
Base réduite (2000)	-	-	$q^{3/2}$	$q^{8/5}$
Single large prime (2003)	-	-	$q^{10/7}$	$q^{14/9}$
Double large prime (2005)	-	-	$q^{4/3}$	$q^{3/2}$
Bas degré (2006)	-	-	q	

Compétition entre le genre 1 (courbes elliptiques) et 2 (hyperelliptiques).

Tout dépend de la vitesse des opérations dans le groupe et des possibilités de construction de bonnes courbes.

Comparaison des vitesses de calcul (P. Gaudry)

eBats (ECRYPT Benchmarking of Asymmetric Systems) : temps en cycles CPU.

	$g = 1,\ p = 2^{255} - 19$	$g = 2,\ p = 2^{127} - 739$
Opteron K8	310.000	296.000
Core2	386.000	405.000
Pentium 4	3.570.000	3.300.000
Pentium M	1.708.000	2.000.000

	$g = 1,\ q = 2^{251}$	$g = 2,\ q = 2^{113}$
Opteron K8	1.400.000	1.200.000
Core2	888.000	687.000
Pentium 4	3.085.000	2.815.000
Pentium M	2.480.000	2.020.000

Comparaison des vitesses de calcul (P. Gaudry)

eBats (ECRYPT Benchmarking of Asymmetric Systems) : temps en cycles CPU.

	$g = 1,\ p = 2^{255} - 19$	$g = 2,\ p = 2^{127} - 739$
Opteron K8	310.000	296.000
Core2	386.000	405.000
Pentium 4	3.570.000	3.300.000
Pentium M	1.708.000	2.000.000

	$g = 1,\ q = 2^{251}$	$g = 2,\ q = 2^{113}$
Opteron K8	1.400.000	1.200.000
Core2	888.000	687.000
Pentium 4	3.085.000	2.815.000
Pentium M	2.480.000	2.020.000

Comparaisons réalisées avant le modèle d'Edwards . . .

Les courbes elliptiques

$$E/\mathbb{F}_q : f(x,y) := y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0.$$

L'ensemble qui nous intéresse est

$$E(\mathbb{F}_q) = \{(x,y) \in \mathbb{F}_q^2 \text{ tels que } f(x,y) = 0\} \cup \{O_E\}.$$

C'est un groupe (voir l'exposé de Laurent).

Rappel : on veut que le cardinal du groupe $E(\mathbb{F}_q)$ ait un gros facteur premier.

Construction de bonnes courbes elliptiques

Rappel : on veut que le cardinal du groupe $E(\mathbb{F}_q)$ ait un gros facteur premier.

basiques	Méthodes adiques (E varie)	CM (q varie)
comptage algo $\sqrt{\ }$ extension	l-adique (p grand) relèv. canonique (p petit $= 2$) cohomologique (p petit) déformation (p petit)	sur $\mathbb{C}$ TRC relèvement à la carte

- Comptage : $\#E(\mathbb{F}_p) = 1 + \sum_{i=0}^{p-1} 1 + \left(\frac{f(i)}{p}\right)$ si $E : y^2 = f(x)$.
  Méthode exponentielle praticable jusqu'à $p \approx 2^{30}$.

- Comptage : $\#E(\mathbb{F}_p) = 1 + \sum_{i=0}^{p-1} 1 + \left(\frac{f(i)}{p}\right)$ si $E : y^2 = f(x)$.
  Méthode exponentielle praticable jusqu'à $p \approx 2^{30}$.
- Algorithme $\sqrt{\ }$: si on sait que si l'ordre N d'un groupe abélien satisfait $B < N < C$ alors il existe un algorithme probabiliste pour le calculer en $\mathcal{O}(\sqrt{C-B})$. Bornes de Weil $\rightsquigarrow \mathcal{O}(q^{1/4})$.

"Méthodes basiques"

- Comptage : $\#E(\mathbb{F}_p) = 1 + \sum_{i=0}^{p-1} 1 + \left(\frac{f(i)}{p}\right)$ si $E : y^2 = f(x)$. Méthode exponentielle praticable jusqu'à $p \approx 2^{30}$.
- Algorithme $\sqrt{}$: si on sait que si l'ordre N d'un groupe abélien satisfait $B < N < C$ alors il existe un algorithme probabiliste pour le calculer en $\mathcal{O}(\sqrt{C-B})$. Bornes de Weil $\rightsquigarrow \mathcal{O}(q^{1/4})$.
- Par extension : Si $\#E(\mathbb{F}_q) = q + 1 + a$, on écrit $X^2 + aX + q = (X - \alpha)(X - \beta)$ et

$$\#E(\mathbb{F}_{q^k}) = 1 + q^k - (\alpha^k + \beta^k).$$

Les dangers des extensions

La descente de Weil : pour $E/\mathbb{F}_{q^k}$, construire $C/\mathbb{F}_q$ de genre petit et un morphisme $\phi : C \to E$ sur $\mathbb{F}_{q^k}$. Puis transférer le DLP par

$$N_{\mathbb{F}_{q^k}/\mathbb{F}_q} \circ \phi^* : E(\mathbb{F}_{q^k}) \to \mathrm{Jac}(C)(\mathbb{F}_q).$$

Les dangers des extensions

La descente de Weil : pour $E/\mathbb{F}_{q^k}$, construire $C/\mathbb{F}_q$ de genre petit et un morphisme $\phi : C \to E$ sur $\mathbb{F}_{q^k}$. Puis transférer le DLP par

$$N_{\mathbb{F}_{q^k}/\mathbb{F}_q} \circ \phi^* : E(\mathbb{F}_{q^k}) \to \mathrm{Jac}(C)(\mathbb{F}_q).$$

En pratique :

- Menezes, Qu : échoue pour toutes les courbes crypto définies sur $\mathbb{F}_{2^n}$ pour $n \in [160, 600]$ premier.

Les dangers des extensions

La descente de Weil : pour $E/\mathbb{F}_{q^k}$, construire $C/\mathbb{F}_q$ de genre petit et un morphisme $\phi : C \to E$ sur $\mathbb{F}_{q^k}$. Puis transférer le DLP par

$$N_{\mathbb{F}_{q^k}/\mathbb{F}_q} \circ \phi^* : E(\mathbb{F}_{q^k}) \to \mathrm{Jac}(C)(\mathbb{F}_q).$$

En pratique :

- Menezes, Qu : échoue pour toutes les courbes crypto définies sur $\mathbb{F}_{2^n}$ pour $n \in [160, 600]$ premier.
- Menezes, Teske, Weng (resp. Hess) : pour $2^{94}/2^{162}$ (resp. $2^{123}/2^{156}$) classes d'isomorphismes de c.e. sur $\mathbb{F}_{2^{23 \cdot 7}}$ (resp. $\mathbb{F}_{2^{31 \cdot 5}}$) réduit le DLP à 2^{48} (resp. 2^{45}) étapes (pour des courbes hyperelliptiques de genre 8 (resp. 31) sur $\mathbb{F}_{2^{23}}$ (resp. $\mathbb{F}_{2^5}$)).

Les dangers des extensions

La descente de Weil : pour $E/\mathbb{F}_{q^k}$, construire $C/\mathbb{F}_q$ de genre petit et un morphisme $\phi : C \to E$ sur $\mathbb{F}_{q^k}$. Puis transférer le DLP par

$$N_{\mathbb{F}_{q^k}/\mathbb{F}_q} \circ \phi^* : E(\mathbb{F}_{q^k}) \to \mathrm{Jac}(C)(\mathbb{F}_q).$$

En pratique :

- Menezes, Qu : échoue pour toutes les courbes crypto définies sur $\mathbb{F}_{2^n}$ pour $n \in [160, 600]$ premier.
- Menezes, Teske, Weng (resp. Hess) : pour $2^{94}/2^{162}$ (resp. $2^{123}/2^{156}$) classes d'isomorphismes de c.e. sur $\mathbb{F}_{2^{23 \cdot 7}}$ (resp. $\mathbb{F}_{2^{31 \cdot 5}}$) réduit le DLP à 2^{48} (resp. 2^{45}) étapes (pour des courbes hyperelliptiques de genre 8 (resp. 31) sur $\mathbb{F}_{2^{23}}$ (resp. $\mathbb{F}_{2^5}$)).
- Diem : si $(q, 6) = 1$ alors il existe un transfert pour toutes les c.e. sur $\mathbb{F}_q$ considérées sur une extension de degré 7.

Autres dangers connus ?

- L'attaque par transfert (Smart-Araki-Satoh-Semaev) : lorsque $\#E(\mathbb{F}_q) = q$ il existe une attaque en $\mathcal{O}(\log(q))$. Deux interprétations :
  - isomorphisme avec les différentielles logarithmiques (Rück).
  - relèvement (non canonique !) dans $\mathcal{E}_1(\mathbb{Q}_p)$ (Couveignes).

  Rq. : toutes les autres idées de relèvement sont pour l'instant des échecs (voir Silverman ECC07).

- L'attaque par transfert (Smart-Araki-Satoh-Semaev) : lorsque $\#E(\mathbb{F}_q) = q$ il existe une attaque en $\mathcal{O}(\log(q))$. Deux interprétations :
  - isomorphisme avec les différentielles logarithmiques (Rück).
  - relèvement (non canonique !) dans $\mathcal{E}_1(\mathbb{Q}_p)$ (Couveignes).

  Rq. : toutes les autres idées de relèvement sont pour l'instant des échecs (voir Silverman ECC07).
- L'attaque par l'accouplement de Tate-Lichtenbaum (Menezes-Okamoto-Vanstone) : soit l premier et k tel que $l | q^k - 1$.

$$T_l : E(\mathbb{F}_q)[l] \times E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*[l].$$

  Si $k < 20$ on a une attaque plus rapide pour le logarithme discret dans le sous-groupe d'ordre l. C'est le cas des courbes supersingulières ($k \leq 6$) et des courbes telles que $\#E(\mathbb{F}_q) = q - 1$.

Méthode l-adique (Schoof 85)

Résultat : $\pi_E : (x,y) \mapsto (x^q, y^q)$ satisfait $\boxed{\pi_E^2 + a\pi_E + q = 0}$.

Méthode l-adique (Schoof 85)

Résultat : $\pi_E : (x,y) \mapsto (x^q, y^q)$ satisfait $\boxed{\pi_E^2 + a\pi_E + q = 0}$.

1. $|a| \leq 2\sqrt{q} \rightsquigarrow$ déterminer $\#E(\mathbb{F}_q)$ modulo $L = \prod l_i^{e_i} > 4\sqrt{q}$ ($\boxed{\text{TRC}}$).

Méthode l-adique (Schoof 85)

Résultat : $\pi_E : (x, y) \mapsto (x^q, y^q)$ satisfait $\boxed{\pi_E^2 + a\pi_E + q = 0}$.

1. $|a| \leq 2\sqrt{q} \rightsquigarrow$ déterminer $\#E(\mathbb{F}_q)$ modulo $L = \prod l_i^{e_i} > 4\sqrt{q}$ ($\boxed{\text{TRC}}$).
2. Soit $l \neq p$ et $P \in E[l]$. Si on trouve t tel que

$$\pi_E(P)^2 + qP = -t\pi_E(P)$$

on a $(a - t)\pi_E(P) = O_E$ donc $a \equiv t \pmod{l}$.

Méthode l-adique (Schoof 85)

Résultat : $\pi_E : (x, y) \mapsto (x^q, y^q)$ satisfait $\boxed{\pi_E^2 + a\pi_E + q = 0}$.

1. $|a| \leq 2\sqrt{q} \rightsquigarrow$ déterminer $\#E(\mathbb{F}_q)$ modulo $L = \prod l_i^{e_i} > 4\sqrt{q}$ ($\boxed{\text{TRC}}$).
2. Soit $l \neq p$ et $P \in E[l]$. Si on trouve t tel que

$$\pi_E(P)^2 + qP = -t\pi_E(P)$$

on a $(a - t)\pi_E(P) = O_E$ donc $a \equiv t \pmod{l}$.

En pratique : calcul du polynôme de division $\phi_l(x)$ de degré $(l^2 - 1)/2$; égalité des endomorphismes $\pi_E^2 + q$ et $a\pi_E$ dans l'algèbre

$$\mathbb{F}_q[x, y]/(\phi_l(x), f(x, y)).$$

Institut de Mathématiques de Luminy

Méthode l-adique (Schoof 85)

Résultat : $\pi_E : (x,y) \mapsto (x^q, y^q)$ satisfait $\boxed{\pi_E^2 + a\pi_E + q = 0}$.

1. $|a| \leq 2\sqrt{q} \rightsquigarrow$ déterminer $\#E(\mathbb{F}_q)$ modulo $L = \prod l_i^{e_i} > 4\sqrt{q}$ ($\boxed{\text{TRC}}$).
2. Soit $l \neq p$ et $P \in E[l]$. Si on trouve t tel que

$$\pi_E(P)^2 + qP = -t\pi_E(P)$$

on a $(a-t)\pi_E(P) = O_E$ donc $a \equiv t \pmod{l}$.

En pratique : calcul du polynôme de division $\phi_l(x)$ de degré $(l^2-1)/2$; égalité des endomorphismes $\pi_E^2 + q$ et $a\pi_E$ dans l'algèbre

$$\mathbb{F}_q[x,y]/(\phi_l(x), f(x,y)).$$

Complexité : $\widetilde{\mathcal{O}}(\log^5 q)$.

Amélioration : Schoof-Elkies-Atkin

Idée : utiliser l-ième polynôme modulaire $\boxed{\psi_l(x, y)}$ de degré $l + 1$.

Amélioration : Schoof-Elkies-Atkin

Idée : utiliser l-ième polynôme modulaire $\boxed{\psi_l(x,y)}$ de degré $l+1$.

- Si $\psi_l(x,j_E)$ a une racine dans $\mathbb{F}_q$, il existe un sous-groupe $C_l \in E[l](\mathbb{F}_q)$ et on remplace $\phi_l(x)$ par

$$g_l(x) = \prod_{\pm P \in C_l \setminus \{O_E\}} (x - x_P).$$

$g_l(x)$ est calculé grâce au développement de $\wp$ et des coefficients de la courbe E/C_l.

Amélioration : Schoof-Elkies-Atkin

Idée : utiliser l-ième polynôme modulaire $\boxed{\psi_l(x,y)}$ de degré $l+1$.

- Si $\psi_l(x, j_E)$ a une racine dans $\mathbb{F}_q$, il existe un sous-groupe $C_l \in E[l](\mathbb{F}_q)$ et on remplace $\phi_l(x)$ par
$$g_l(x) = \prod_{\pm P \in C_l \setminus \{O_E\}} (x - x_P).$$
$g_l(x)$ est calculé grâce au développement de $\wp$ et des coefficients de la courbe E/C_l.
- Sinon il existe $r > 1$ tel que $\psi_l(x, j_E) | x^{q^r} - x$ et une racine r-ième ζ tel que $a^2 \equiv q(\zeta + \zeta^{-1})^2 \pmod{l}$. $\rightsquigarrow$ $\phi(r)$ possibilités pour $a \pmod{l}$. Pas de bébé-Pas de géant pour décider.

Autres améliorations et complexités

Amélioration (Enge) : d'autres modèles pour $X_0(l) \rightsquigarrow$ polynôme $\psi_l(x,y)$ avec coefficients plus petits ou degré moindre en y.
Complexité : $\mathcal{O}(l^3 \log^4 l \log\log l)$ (quasi-linéaire en la taille de $\psi_l(x,y)$).

Autres améliorations et complexités

Amélioration (Enge) : d'autres modèles pour $X_0(l) \rightsquigarrow$ polynôme $\psi_l(x, y)$ avec coefficients plus petits ou degré moindre en y.
Complexité : $\mathcal{O}(l^3 \log^4 l \log\log l)$ (quasi-linéaire en la taille de $\psi_l(x, y)$).

Amélioration (Couveignes, Lercier, Morain) : lorsque $q = p^n$ avec p petit.

Autres améliorations et complexités

Amélioration (Enge) : d'autres modèles pour $X_0(l) \rightsquigarrow$ polynôme $\psi_l(x,y)$ avec coefficients plus petits ou degré moindre en y.
Complexité : $\mathcal{O}(l^3 \log^4 l \operatorname{llog} l)$ (quasi-linéaire en la taille de $\psi_l(x,y)$).

Amélioration (Couveignes, Lercier, Morain) : lorsque $q = p^n$ avec p petit.

Complexité : $\mathcal{O}(\log^4 q)$ en temps et $\mathcal{O}(\log^2 q)$ en espace.
Records : Vercauteren $q = 2^{1999}$ et Enge-Gaudry-Morain $q = 10^{2099} + 6243$.

Nouvelles idées ? (Couveignes-de Jong-Edixhoven-Merkl-Bosman) : calcul en temps polynomial de coefficients de formes modulaires.

Relèvement ?

Problème : en caractéristique p, $d(x^p)/dx = 0$.

Relèvement ?

Problème : en caractéristique p, $d(x^p)/dx = 0$.

Solution : $\boxed{\text{relever}}$ en caractéristique 0.

Relèvement ?

Problème : en caractéristique p, $d(x^p)/dx = 0$.

Solution : $\boxed{\text{relever}}$ en caractéristique 0.

En pratique : $\mathbb{F}_p \rightsquigarrow \mathbb{Z}_p \subset \mathbb{Q}_p$ corps p-adique. On a $\mathbb{Z}_p/(p) = \mathbb{F}_p$.

Relèvement ?

Problème : en caractéristique p, $d(x^p)/dx = 0$.

Solution : $\boxed{\text{relever}}$ en caractéristique 0.

En pratique : $\mathbb{F}_p \rightsquigarrow \mathbb{Z}_p \subset \mathbb{Q}_p$ corps p-adique. On a $\mathbb{Z}_p/(p) = \mathbb{F}_p$.

Plus généralement $\mathbb{F}_q \rightsquigarrow \mathbb{Z}_q \subset \mathbb{Q}_q$ extension (non-ramifiée) de degré n de $\mathbb{Q}_p$.

On note aussi $\sigma \in \mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$ (substitution de Frobenius) tel que

$$\widetilde{\sigma(x)} = \tilde{x}^p.$$

Institut de Mathématiques de Luminy

Autour du relèvement canonique

Idée : relever en une courbe particulière + action sur espace classique.

Autour du relèvement canonique

Idée : relever en une courbe particulière + action sur espace classique.

Résultat : pour toute courbe elliptique (ordinaire) $E/\mathbb{F}_q$ il existe un unique relèvement canonique $\boxed{\mathcal{E}/\mathbb{Q}_q}$ tel que $\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E)$.

Autour du relèvement canonique

Idée : relever en une courbe particulière + action sur espace classique.

Résultat : pour toute courbe elliptique (ordinaire) $E/\mathbb{F}_q$ il existe un unique relèvement canonique $\boxed{\mathcal{E}/\mathbb{Q}_q}$ tel que $\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E)$.

1. relever Frobenius π_E en $\pi_{\mathcal{E}}$;

Autour du relèvement canonique

Idée : relever en une courbe particulière + action sur espace classique.

Résultat : pour toute courbe elliptique (ordinaire) $E/\mathbb{F}_q$ il existe un unique relèvement canonique $\boxed{\mathcal{E}/\mathbb{Q}_q}$ tel que $\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E)$.

1. relever Frobenius π_E en $\pi_{\mathcal{E}}$;
2. action sur une différentielle régulière : $\pi_{\mathcal{E}}^*(w) = cw$;

Autour du relèvement canonique

Idée : relever en une courbe particulière + action sur espace classique.

Résultat : pour toute courbe elliptique (ordinaire) $E/\mathbb{F}_q$ il existe un unique relèvement canonique $\boxed{\mathcal{E}/\mathbb{Q}_q}$ tel que $\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E)$.

1. relever Frobenius π_E en $\pi_{\mathcal{E}}$;
2. action sur une différentielle régulière : $\pi_{\mathcal{E}}^*(w) = cw$;
3. $\#E(\mathbb{F}_q) = q + 1 - (c + q/c)$.

Idée : relever en une courbe particulière + action sur espace classique.

Résultat : pour toute courbe elliptique (ordinaire) $E/\mathbb{F}_q$ il existe un unique relèvement canonique $\boxed{\mathcal{E}/\mathbb{Q}_q}$ tel que $\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E)$.

1. relever Frobenius π_E en $\pi_{\mathcal{E}}$;
2. action sur une différentielle régulière : $\pi_{\mathcal{E}}^*(w) = cw$;
3. $\#E(\mathbb{F}_q) = q + 1 - (c + q/c)$.

En pratique : autant pour le calcul de $\mathcal{E}$ que de $\pi_{\mathcal{E}}$, il faut que $q = p^n$ avec p petit afin de :

1. factoriser π_E et $\pi_{\mathcal{E}}$ en n isogénies de degré p.

Autour du relèvement canonique

Idée : relever en une courbe particulière + action sur espace classique.

Résultat : pour toute courbe elliptique (ordinaire) $E/\mathbb{F}_q$ il existe un unique relèvement canonique $\boxed{\mathcal{E}/\mathbb{Q}_q}$ tel que $\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E)$.

1. relever Frobenius π_E en $\pi_{\mathcal{E}}$;
2. action sur une différentielle régulière : $\pi_{\mathcal{E}}^*(w) = cw$;
3. $\#E(\mathbb{F}_q) = q + 1 - (c + q/c)$.

En pratique : autant pour le calcul de $\mathcal{E}$ que de $\pi_{\mathcal{E}}$, il faut que $q = p^n$ avec p petit afin de :

1. factoriser π_E et $\pi_{\mathcal{E}}$ en n isogénies de degré p.
2. chercher un invariant $j \in \mathbb{Q}_q$ solution de l'équation modulaire

$$\psi_p(j, j^\sigma) = 0.$$

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	relève tous les $\mathcal{E}^{\sigma^i}$ (pas de calcul de σ)

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	$p = 2, 3$

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	nouveau calcul de $\ker \mathrm{Fr}_{\mathcal{E}} : \mathcal{E} \rightarrow \mathcal{E}^{\sigma}$

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3), \mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	relève une seule courbe

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	isogénie très simple (formule ana. $\boxed{\text{AGM}}$)

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3), \mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3), \mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)

Institut de Mathématiques de Luminy

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3), \mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3), \mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	calcul rapide de σ

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3), \mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3), \mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5}), \mathcal{O}(n^2)$

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	base gaussienne normale (BGN)

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	combine AGM et SST en modifiant ψ_p

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)

Institut de Mathématiques de Luminy

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	BGN + meilleur Newton

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	$\widetilde{\mathcal{O}}(n^2)$,$\mathcal{O}(n^2)$

Institut de Mathématiques de Luminy

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	$\widetilde{\mathcal{O}}(n^2)$,$\mathcal{O}(n^2)$
02 : Harley ($p = 2$)	Newton general + calcul de la norme

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3),\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3),\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5}),\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	$\widetilde{\mathcal{O}}(n^2),\mathcal{O}(n^2)$
02 : Harley ($p = 2$)	" (pour tout n) ©.

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	$\widetilde{\mathcal{O}}(n^2)$,$\mathcal{O}(n^2)$
02 : Harley ($p = 2$)	" (pour tout n) ©.
03 : Kohel ($X_0(p)$ de genre 0)	modulaire AGM $p = 3, 5, 7, 13$

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	$\widetilde{\mathcal{O}}(n^2)$,$\mathcal{O}(n^2)$
02 : Harley ($p = 2$)	" (pour tout n) ©.
03 : Kohel ($X_0(p)$ de genre 0)	"

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	$\widetilde{\mathcal{O}}(n^2)$,$\mathcal{O}(n^2)$
02 : Harley ($p = 2$)	" (pour tout n) ©.
03 : Kohel ($X_0(p)$ de genre 0)	"
04 : Gustavsen-Ranestad	AGM géométrique $p = 3$

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	$\widetilde{\mathcal{O}}(n^2)$,$\mathcal{O}(n^2)$
02 : Harley ($p = 2$)	" (pour tout n) ©.
03 : Kohel ($X_0(p)$ de genre 0)	"
04 : Gustavsen-Ranestad	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\tilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\tilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\tilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	$\tilde{\mathcal{O}}(n^2)$,$\mathcal{O}(n^2)$
02 : Harley ($p = 2$)	" (pour tout n) ©.
03 : Kohel ($X_0(p)$ de genre 0)	"
04 : Gustavsen-Ranestad	$\tilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
06- : Carls-Kohel-Lubicz	AGM géométrique $p > 2$

Les algorithmes et complexité

99 : Satoh ($p > 3$, $X(1)$)	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^3)$
Fouquet-Gaudry-Harley	"
Skjernaa	"
Vercauteren	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
00 : Mestre ($p = 2$, $X_0(8)$)	" (code très simple, $\pi_{\mathcal{E}}$ gratuit)
Satoh-Skjernaa-Takachi ($p = 2$)	$\widetilde{\mathcal{O}}(n^{2.5})$,$\mathcal{O}(n^2)$
Kim et *al.* ($p = 2$)	" (sans précalcul)
01 : Gaudry MSST ($p = 2$)	" (constante car degré plus petit)
Lercier-Lubicz ($p = 2$)	$\widetilde{\mathcal{O}}(n^2)$,$\mathcal{O}(n^2)$
02 : Harley ($p = 2$)	" (pour tout n) ©.
03 : Kohel ($X_0(p)$ de genre 0)	"
04 : Gustavsen-Ranestad	$\widetilde{\mathcal{O}}(n^3)$,$\mathcal{O}(n^2)$
06- : Carls-Kohel-Lubicz	?

En temps de calcul (Vercauteren sur $\mathbb{F}_{2^n}$)

En secondes sur un processeur AMD XP 1700+ (Linux RedHat 7.1).

n	FGH	SKJ	VER	AGM	SST	MSST	HAR
144	3.99	2.89	1.91	0.57	0.13	0.06	0.06
192	6.04	4.93	3.22	0.88	0.26	0.08	0.08
480	205.3	157.9	106.5	34.5	3.56	2.03	1.87

n	KIM	LELU
148	0.04	0.02
466	0.872	0.374

Record : Lercier-Lubicz (02) : $n = 100002$.

Méthodes cohomologiques

Idée : relever en une courbe 'quelconque' $X : y^2 = F(x)$ et action sur un espace compliqué :

$$A^\dagger = \mathbb{Q}_q[x, y, y^{-1}]^\dagger / (y^2 - F(x))$$

où $\mathbb{Q}_q[x, y, y^{-1}]^\dagger$ est l'algèbre des séries formelles + propriété de convergence.

Méthodes cohomologiques

Idée : relever en une courbe 'quelconque' $X : y^2 = F(x)$ et action sur un espace compliqué :

$$A^\dagger = \mathbb{Q}_q[x, y, y^{-1}]^\dagger / (y^2 - F(x))$$

où $\mathbb{Q}_q[x, y, y^{-1}]^\dagger$ est l'algèbre des séries formelles + propriété de convergence.

Relèvement du Frobenius :

$$\mathcal{F} : (x, y) \to (x^p, y^p(1 + \frac{F^\sigma(x^p) - F(x)^p}{y^{2p}})^{1/2}).$$

Méthodes cohomologiques

Idée : relever en une courbe 'quelconque' $X : y^2 = F(x)$ et action sur un espace compliqué :

$$A^\dagger = \mathbb{Q}_q[x, y, y^{-1}]^\dagger / (y^2 - F(x))$$

où $\mathbb{Q}_q[x, y, y^{-1}]^\dagger$ est l'algèbre des séries formelles + propriété de convergence.

Relèvement du Frobenius :

$$\mathcal{F} : (x, y) \to (x^p, y^p(1 + \frac{F^\sigma(x^p) - F(x)^p}{y^{2p}})^{1/2}).$$

Formule de trace :

$$\# E(\mathbb{F}_q) = 1 + q - \mathrm{tr}(q\mathcal{F}^{-1} | H^1_{\mathrm{MW}}(X))$$

(MW : cohomologie de Monsky-Washnitzer).

En pratique

- Algorithme de Kedlaya (p>2) : $\widetilde{\mathcal{O}}(pg^4 n^3)$ en temps et $\widetilde{\mathcal{O}}(pg^3 n^3)$ en espace.
- Denef-Vercauteren ($p = 2$).
- De p à $\sqrt{p}$ en temps : Bostan-Gaudry-Schost, Harvey.
- Variantes : cohomologie de Dwork-Reich (Lauder et Wan), rigide, cristalline.

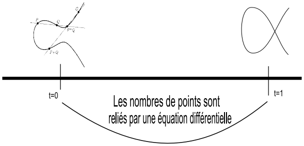
En pratique

- Algorithme de Kedlaya (p>2) : $\widetilde{\mathcal{O}}(pg^4n^3)$ en temps et $\widetilde{\mathcal{O}}(pg^3n^3)$ en espace.
- Denef-Vercauteren ($p = 2$).
- De p à $\sqrt{p}$ en temps : Bostan-Gaudry-Schost, Harvey.
- Variantes : cohomologie de Dwork-Reich (Lauder et Wan), rigide, cristalline.

Non compétitif avec le relèvement canonique. Peut-être utile pour p médium par descente de Weil car meilleure dépendance en p et en g.

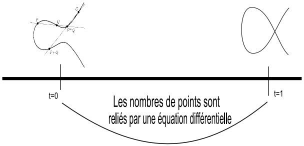
Nouvelle piste : la déformation

Fig.: Déformation de Lauder



Nouvelle piste : la déformation

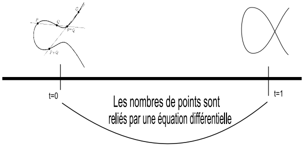
Fig.: Déformation de Lauder



- Gerkmann et Hubrechts (Lauder+Kedlaya) : complexité en espace $\widetilde{\mathcal{O}}(pg^4 n^2)$.

Nouvelle piste : la déformation

Fig.: Déformation de Lauder



- Gerkmann et Hubrechts (Lauder+Kedlaya) : complexité en espace $\widetilde{\mathcal{O}}(pg^4 n^2)$.
- Hubrechts (fév.08) : (Lauder+Kedlaya+ norme rapide) $\widetilde{\mathcal{O}}(n^2)$ en temps.

Exemples en s. (Hubrechts) : AMD Athlon 64 3000+.

$p \setminus n$	50	500	4000
3	.15	16.58	4252
5	.26	36.55	-
7	1.76	167.56	-

Multiplication complexe (CM)

Idée : trouver $E/\overline{\mathbb{Q}}$ tq $\#(E \pmod p)$ est facile à calculer.

- soit $E/\overline{\mathbb{Q}}$ telle que $\mathbb{Z} \subsetneq \mathrm{End}(E) = O_K \subset K = \mathbb{Q}(\sqrt{-d})$ avec O_K l'anneau des entiers de K et $1 < d \equiv 3 \pmod 4$.

Multiplication complexe (CM)

Idée : trouver $E/\overline{\mathbb{Q}}$ tq $\#(E \pmod p)$ est facile à calculer.

- soit $E/\overline{\mathbb{Q}}$ telle que $\mathbb{Z} \subsetneq \mathrm{End}(E) = O_K \subset K = \mathbb{Q}(\sqrt{-d})$ avec O_K l'anneau des entiers de K et $1 < d \equiv 3 \pmod 4$.
- Soit p premier grand tel que $4p = x^2 + dy^2$ (algo Cornacchia).

Multiplication complexe (CM)

Idée : trouver $E/\overline{\mathbb{Q}}$ tq $\#(E \pmod p)$ est facile à calculer.

- soit $E/\overline{\mathbb{Q}}$ telle que $\mathbb{Z} \subsetneq \mathrm{End}(E) = O_K \subset K = \mathbb{Q}(\sqrt{-d})$ avec O_K l'anneau des entiers de K et $1 < d \equiv 3 \pmod 4$.
- Soit p premier grand tel que $4p = x^2 + dy^2$ (algo Cornacchia).
- Alors $E \pmod p$ a pour cardinal $\boxed{p + 1 \pm x}$.

Multiplication complexe (CM)

Idée : trouver $E/\overline{\mathbb{Q}}$ tq $\#(E \pmod p)$ est facile à calculer.

- soit $E/\overline{\mathbb{Q}}$ telle que $\mathbb{Z} \subsetneq \mathrm{End}(E) = O_K \subset K = \mathbb{Q}(\sqrt{-d})$ avec O_K l'anneau des entiers de K et $1 < d \equiv 3 \pmod 4$.
- Soit p premier grand tel que $4p = x^2 + dy^2$ (algo Cornacchia).
- Alors $E \pmod p$ a pour cardinal $\boxed{p + 1 \pm x}$.

Ex. : $E : y^2 = x(x^2 - 21x + 112)$ avec $d = 7$.
$4 \cdot 11 = 4^2 + 7 \cdot 2^2$ et $\#E(\mathbb{F}_{11}) = 16 = 11 + 1 + 4$.

Rem. : on veut d grand.

Question : comment obtenir E (ou $E \pmod p$) ?

Soit $K = \mathbb{Q}(\sqrt{-d})$ et I un idéal de O_K.

$I \subset \mathbb{C}$ est un réseau et $E_I = \mathbb{C}/I \simeq \mathbb{C}/\mathbb{Z} + \tau_I\mathbb{Z}$ est une courbe elliptique telle que $\mathrm{End}(E_I) = O_K$.

Polynôme de classes de Hilbert :

$$H_d(X) = \prod_{I \in Cl(O_K)} (X - j(\tau_I)) \in \mathbb{Z}[X]$$

avec $j(\tau) = 1/q + 744 + 196884q + \ldots$ et $q = \exp(2i\pi\tau)$.

Institut de Mathématiques de Luminy

En pratique

- idéaux $\iff$ formes quadratiques (réduites) $ax^2 + bx + c$ de discriminant d et $\tau = \frac{b+\sqrt{-d}}{2a}$.

En pratique

- idéaux $\iff$ formes quadratiques (réduites) $ax^2 + bx + c$ de discriminant d et $\tau = \frac{b+\sqrt{-d}}{2a}$.
- Evaluation des j (Enge) :
  1. utilisation de

$$\eta = q^{1/24}(1 + \sum_{n=1}^{\infty}(-1)^n(q^{n(3n-1)/2} + q^{n(3n+1)/2})).$$

Institut de Mathématiques de Luminy

En pratique

- idéaux $\Longleftrightarrow$ formes quadratiques (réduites) $ax^2 + bx + c$ de discriminant d et $\tau = \frac{b+\sqrt{-d}}{2a}$.
- Evaluation des j (Enge) :
  1. utilisation de
  $$\eta = q^{1/24}(1 + \sum_{n=1}^{\infty}(-1)^n(q^{n(3n-1)/2} + q^{n(3n+1)/2})).$$
  2. évaluation multi-points.

En pratique

- idéaux $\iff$ formes quadratiques (réduites) $ax^2 + bx + c$ de discriminant d et $\tau = \frac{b+\sqrt{-d}}{2a}$.
- Evaluation des j (Enge) :
  1. utilisation de
  $$\eta = q^{1/24}(1 + \sum_{n=1}^{\infty}(-1)^n(q^{n(3n-1)/2} + q^{n(3n+1)/2})).$$
  2. évaluation multi-points.
  3. itérations de Newton sur l'AGM (avec l'algo de Dupont).

En pratique

- idéaux $\iff$ formes quadratiques (réduites) $ax^2 + bx + c$ de discriminant d et $\tau = \frac{b+\sqrt{-d}}{2a}$.
- Evaluation des j (Enge) :
  1. utilisation de
  $$\eta = q^{1/24}(1 + \sum_{n=1}^{\infty}(-1)^n(q^{n(3n-1)/2} + q^{n(3n+1)/2})).$$
  2. évaluation multi-points.
  3. itérations de Newton sur l'AGM (avec l'algo de Dupont).
- La hauteur de H_d est élevé : remplacer j par des fonctions de Weber.

Complexité et résultats (Enge)

Sur AMD Opteron 250 à 2.4 Ghz en secondes.

$\deg(H_d)$	5000	20000	100000	
d	69611631	98016239	2093236031	
η	28	1800	270000	$\widetilde{\mathcal{O}}(\lvert d\rvert^{5/4})$
ev. multipoint	110	6500	-	$\mathcal{O}(d \log^{6+o(1)} d)$
AGM	48	2300	260000	$\mathcal{O}(d \log^{5+o(1)} d)$

A un facteur logarithmique près ceci correspond à la complexité d'écriture de la sortie.

Pour le cas 100000 : 3 jours pour 5GB en texte compressé.

TRC (08) (Belding, Bröker, Enge, Lauter)

Idée : calcul de $H_d \pmod{p}$ pour différents p puis TRC.

TRC (08) (Belding, Bröker, Enge, Lauter)

Idée : calcul de $H_d \pmod p$ pour différents p puis TRC.

En pratique :

- Enumeration sur $\mathbb{F}_p$ (Agashe, Lauter, Venkatesan) : $\widetilde{\mathcal{O}}(d^{3/2})$.

TRC (08) (Belding, Bröker, Enge, Lauter)

Idée : calcul de $H_d \pmod p$ pour différents p puis TRC.

En pratique :

- Enumeration sur $\mathbb{F}_p$ (Agashe, Lauter, Venkatesan) : $\widetilde{\mathcal{O}}(d^{3/2})$.
- Le cas p tot. décomposé $(p > d)$:
  1. trouver E avec $\mathrm{End}(E) = O_K$.
  2. calculer $j(E)^{\mathfrak{a}}$ pour $\mathfrak{a} \in Cl(O_K)$.
  3. Retourner $H_d \pmod p = \prod(X - j(E)^{\mathfrak{a}})$.

TRC (08) (Belding, Bröker, Enge, Lauter)

Idée : calcul de $H_d \pmod p$ pour différents p puis TRC.

En pratique :

- Enumeration sur $\mathbb{F}_p$ (Agashe, Lauter, Venkatesan) : $\widetilde{\mathcal{O}}(d^{3/2})$.
- Le cas p tot. décomposé ($p > d$) :
  1. trouver E avec $\mathrm{End}(E) = O_K$.
  2. calculer $j(E)^{\mathfrak{a}}$ pour $\mathfrak{a} \in Cl(O_K)$.
  3. Retourner $H_d \pmod p = \prod(X - j(E)^{\mathfrak{a}})$.
- Le cas p inerte (p petit) :
  1. calcul de la liste des j supersinguliers sur $\mathbb{F}_{p^2}$ avec leur anneau d'endomorphismes dans $\mathcal{A}_{p,\infty}$.
  2. calcul d'un plongement optimal $s : O_K \to \mathcal{A}_{p,\infty}$ et $R \supset s(O_K)$ un ordre maximal.
  3. trouver E dans la liste avec $\mathrm{End}(E) = R$.
  4. retourner $H_d \pmod p = \prod(X - j(E)^{\mathfrak{a}})$.

TRC (08) (Belding, Bröker, Enge, Lauter)

Idée : calcul de $H_d \pmod p$ pour différents p puis TRC.

En pratique :

- Enumeration sur $\mathbb{F}_p$ (Agashe, Lauter, Venkatesan) : $\widetilde{\mathcal{O}}(d^{3/2})$.
- Le cas p tot. décomposé ($p > d$) :
  1. trouver E avec $\mathrm{End}(E) = O_K$.
  2. calculer $j(E)^{\mathfrak{a}}$ pour $\mathfrak{a} \in Cl(O_K)$.
  3. Retourner $H_d \pmod p = \prod (X - j(E)^{\mathfrak{a}})$.
- Le cas p inerte (p petit) :
  1. calcul de la liste des j supersinguliers sur $\mathbb{F}_{p^2}$ avec leur anneau d'endomorphismes dans $\mathcal{A}_{p,\infty}$.
  2. calcul d'un plongement optimal $s : O_K \to \mathcal{A}_{p,\infty}$ et $R \supset s(O_K)$ un ordre maximal.
  3. trouver E dans la liste avec $\mathrm{End}(E) = R$.
  4. retourner $H_d \pmod p = \prod (X - j(E)^{\mathfrak{a}})$.

Complexité : GRH ($\mathcal{O}(d \log^{7+o(1)} d)$) ; heuristique ($\mathcal{O}(d \log^{3+o(1)} d)$).

En chiffre : $\deg(H_d) = 100$: 14s (.3s analytique).

Autre piste : relèvement

Idée : sur $\mathbb{F}_q$ une courbe elliptique ordinaire est CM.
Prendre le relèvement canonique $\mathcal{E}$ de $E/\mathbb{F}_q$ $(\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E))$ et de ses conjugués.

Autre piste : relèvement

Idée : sur $\mathbb{F}_q$ une courbe elliptique ordinaire est CM.
Prendre le relèvement canonique $\mathcal{E}$ de $E/\mathbb{F}_q$ $(\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E))$ et de ses conjugués.

En pratique (Couveignes-Henocq) :

- si p est petit, on utilise Satoh ou AGM.
- si p est grand, relèvement avec des endomorphismes friables.

Autre piste : relèvement

Idée : sur $\mathbb{F}_q$ une courbe elliptique ordinaire est CM.
Prendre le relèvement canonique $\mathcal{E}$ de $E/\mathbb{F}_q$ $(\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E))$ et de ses conjugués.

En pratique (Couveignes-Henocq) :

- si p est petit, on utilise Satoh ou AGM.
- si p est grand, relèvement avec des endomorphismes friables.

Rq. : on peut aussi relever les courbes supersingulières.

Complexité : $\mathcal{O}(d \log^4 d)$ (sans problème d'arrondis).

Des courbes à la carte (Bröker, Stevenhagen)

Rappel : π_E satisfait $X^2 + aX + p$ et $N = \#E(\mathbb{F}_p) = 1 + a + p$.

Des courbes à la carte (Bröker, Stevenhagen)

Rappel : π_E satisfait $X^2 + aX + p$ et $N = \#E(\mathbb{F}_p) = 1 + a + p$. Donc $\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{-d})$ avec

$$-d = -f^2\Delta = (N - 1 - p)^2 - 4p = (N + 1 - p)^2 - 4N.$$

Des courbes à la carte (Bröker, Stevenhagen)

Rappel : π_E satisfait $X^2 + aX + p$ et $N = \#E(\mathbb{F}_p) = 1 + a + p$. Donc $\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{-d})$ avec

$$-d = -f^2\Delta = (N-1-p)^2 - 4p = (N+1-p)^2 - 4N.$$

On a donc

$$4N = x^2 + f^2\Delta = 4\alpha\overline{\alpha}, \quad p = N + 1 - x.$$

Des courbes à la carte (Bröker, Stevenhagen)

Rappel : π_E satisfait $X^2 + aX + p$ et $N = \#E(\mathbb{F}_p) = 1 + a + p$. Donc $\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{-d})$ avec

$$-d = -f^2\Delta = (N-1-p)^2 - 4p = (N+1-p)^2 - 4N.$$

On a donc

$$4N = x^2 + f^2\Delta = 4\alpha\overline{\alpha}, \quad p = N + 1 - x.$$

Idée : étant donné N on cherche donc le plus petit Δ tel que il existe $\alpha \in K = \mathbb{Q}(\sqrt{\Delta})$ tq

- $N_{K/\mathbb{Q}}(\alpha) = N$;
- $p = N_{K/\mathbb{Q}}(1-\alpha)$ est premier.

Des courbes à la carte (Bröker, Stevenhagen)

Rappel : π_E satisfait $X^2 + aX + p$ et $N = \#E(\mathbb{F}_p) = 1 + a + p$. Donc $\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{-d})$ avec

$$-d = -f^2\Delta = (N-1-p)^2 - 4p = (N+1-p)^2 - 4N.$$

On a donc

$$4N = x^2 + f^2\Delta = 4\alpha\overline{\alpha}, \quad p = N + 1 - x.$$

Idée : étant donné N on cherche donc le plus petit Δ tel que il existe $\alpha \in K = \mathbb{Q}(\sqrt{\Delta})$ tq

- $N_{K/\mathbb{Q}}(\alpha) = N$;
- $p = N_{K/\mathbb{Q}}(1-\alpha)$ est premier.

Problème : on ne sait pas prouver qu'il existe toujours un $\Delta < \widetilde{\mathcal{O}}(\log^2 N)$.

Des courbes à la carte (Bröker, Stevenhagen)

Rappel : π_E satisfait $X^2 + aX + p$ et $N = \#E(\mathbb{F}_p) = 1 + a + p$. Donc $\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{-d})$ avec

$$-d = -f^2\Delta = (N-1-p)^2 - 4p = (N+1-p)^2 - 4N.$$

On a donc

$$4N = x^2 + f^2\Delta = 4\alpha\overline{\alpha}, \quad p = N + 1 - x.$$

Idée : étant donné N on cherche donc le plus petit Δ tel que il existe $\alpha \in K = \mathbb{Q}(\sqrt{\Delta})$ tq

- $N_{K/\mathbb{Q}}(\alpha) = N$;
- $p = N_{K/\mathbb{Q}}(1-\alpha)$ est premier.

Problème : on ne sait pas prouver qu'il existe toujours un $\Delta < \widetilde{\mathcal{O}}(\log^2 N)$.
Complexité heuristique : $\widetilde{\mathcal{O}}(\log^4 N)$.
Exemple : $N = 10^{2004} + 4863$ en 3 heures sur un PC 2.4 GHz.

Rappel : on veut que le cardinal du groupe $E(\mathbb{F}_q)$ ait un gros facteur premier N. On pose aussi d tel que $\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{-d})$.

"basiques"	Com.	Méthodes adiques	Com.	CM	Com.
comptage	$q^{1/2}$	l-adique	$\log^4 q$	sur $\mathbb{C}$	$d \log^5 d$
algo $\sqrt{}$	$q^{1/4}$	relèv. canonique	$\log^2 q$	TRC	$d \log^3 d$
extension	$\log q$	cohomologique	$\log^3 q$	relèvement	$d \log^4 d$
		déformation	$\log^2 q$	à la carte	$\log^4 N$