Diversité et transparence : choix des courbes elliptiques

Jean-Pierre Flori, Jérôme Plût, Jean-René Reinhard, Martin Ekerå

ANSSI/SDE/ST/LCR

Jeudi 28 mai 2015

I – Introduction

Les courbes elliptiques en cryptographie

- Proposées en 1985 par Koblitz et Miller.
- Fournissent un groupe abélien fini où le logarithme discret est **difficile** (plus que dans les groupes multiplicatifs).
- Standardisées à partir de 2000 :

Année	Courbes	Tailles
2000	NIST	192, 224, 256, 384, 521
2005	Brainpool	160, 192, 224, 256, 320, 384, 512
2010	OSCCA	256
2011	ANSSI	256

- Plus quelques propositions académiques.
- En pratique, on trouve surtout dans la nature les courbes NIST.

Pourquoi les courbes elliptiques ?

- Un outil classique en cryptographie est l'échange de clés de Diffie-Hellman, qui repose sur la relation

$$(g^a)^b = g^{ab} = (g^b)^a,$$

  valable dans le groupe multiplicatif des entiers modulo p.
- La sécurité repose sur le problème du **logarithme discret** : étant donnés g et g^a, il est difficile de calculer a.
- Ce groupe multiplicatif est cependant vulnérable à certaines attaques (« crible algébrique »).
- Solution : augmenter la taille de p...
- ... ou alors, remplacer le groupe multiplicatif par un groupe résistant à ces attaques.

Le groupe des points d'une courbe elliptique

- Une courbe elliptique est donnée par l'équation

$$y^2 = x^3 + ax + b \pmod{p},$$

où p est un nombre premier ($\neq 2, 3$) et a, b sont deux paramètres.

- Les points de la courbe forment un groupe abélien (noté additivement).
- Le cardinal N de ce groupe est environ p ; en fait,

$$|N - (p+1)| \leq 2\sqrt{p}.$$

En général, le groupe des points d'une courbe elliptique se comporte comme un « groupe générique » : le logarithme discret a une complexité exponentielle.

Il est donc possible d'atteindre une sécurité de 128 bits avec une taille de clé de 256 bits.

Pourquoi standardiser ?

En général, le groupe des points d'une courbe elliptique se comporte comme un « groupe générique » : le logarithme discret a une complexité **exponentielle**.

- Plus précisément, la complexité du logarithme discret est dominée par $\sqrt{q}$, où q est le *plus grand diviseur premier* du nombre de points de la courbe.
  - Solution : avoir un nombre de points (presque) premier.
- Certaines courbes particulières sont plus vulnérables : le problème du logarithme discret peut être transféré dans un groupe plus facile.
  - Solution : éviter ces cas particuliers.

Ces solutions sont gourmandes en calculs, il n'est donc pas réaliste d'envisager fabriquer une nouvelle courbe à la volée pour chaque échange.

Deuxième phase de standardisation

Les premières courbes standardisées ont été produites au début des années 2000, c'est-à-dire une fois la recherche dans le domaine suffisamment avancée :

- possibilité de produire des courbes cryptographiques (Schoof, Elkies, Atkin) ;
- identification des classes de courbes faibles.

À notre connaissance, ces courbes sont toujours sûres.

Mais de nouvelles préoccupations sont apparues depuis :

- doutes sur le processus de génération (possibilité de publier une courbe secrètement vulnérable ?) ;
- émergence des attaques latérales (« *side-channel attacks* ») ;
- progrès scientifiques dans des domaines proches (logarithme discret multiplicatif...).

Juin 2015

Le NIST organise un atelier sur le thème de la standardisation des courbes elliptiques.

II – Sécurité

Aspects de la sécurité d'une courbe

Qu'est-ce que qu'une « bonne » courbe pour la cryptographie ?

- Le problème du logarithme discret est difficile.
- Les implémentations de la courbes sont résistantes (par exemple aux attaques par canaux auxiliaires).
- La courbe ne présente aucun signe particulier suspect.
- Il est possible de réaliser des implémentations optimisées.
- La courbe possède des propriétés particulières intéressantes.

Conditions incompatibles

Certaines de ces conditions sont incompatibles entre elles, ce qui peut justifier l'existence de plusieurs (familles de) courbes.

Difficulté du logarithme discret

Si le logarithme discret est facile, alors toute implémentation de la courbe sera faible.

- Il existe des attaques contre des groupes génériques d'ordre N, de complexité $\sqrt{N}$.
- Pour qu'une courbe soit correcte, on exige donc qu'il n'existe pas de meilleure attaque.

Notations

Dans tout ce qui suit, E désigne la courbe d'équation

$$y^2 = x^3 + ax + b$$

définie sur le corps $k = \mathbb{F}_p$, et $N = |E(\mathbb{F}_p)|$. On considère la multiplication $n \cdot P$ pour un scalaire n secret.
On note $\mathcal{P}(X)$ la probabilité d'un événement X comprise, selon le contexte, sur l'ensemble des courbes sur $\mathbb{F}_p$ avec p fixé, ou sur l'ensemble des courbes sur $\mathbb{F}_p$ avec p de taille fixée.

Courbes singulières

Si $\Delta = 4a^3 + 27b^2 = 0$, alors la courbe d'équation $y^2 = x^3 + ax + b$ n'est pas une courbe elliptique : c'est une cubique singulière.
Le groupe des points réguliers est alors isomorphe à un groupe additif ou multiplicatif, et le logarithme discret est sous-exponentiel, voire polynomial.

Il est impératif que $\Delta \neq 0$ (ce qui arrive avec $\mathcal{P} \approx 1$).

Grand sous-groupe premier

- Il existe des attaques génériques de complexité $O(\sqrt{q})$, où q est le plus grand diviseur premier de N.
- Une courbe sûre doit donc avoir $q \approx N$; idéalement, $q = N$.
- Ceci nécessite de calculer N, ce qui est une tâche relativement coûteuse.
- La probabilité qu'une courbe aléatoire ait un ordre premier est approximativement la même que celle qu'un nombre aléatoire de la taille de p soit premier, soit $\mathcal{P} \approx \frac{1}{\log p}$.

- Il est impératif que N ait un grand facteur premier.
- Calculer N est l'une des étapes coûteuses de la génération de la courbe.

Transfert additif ou multiplicatif

- Si $N = p$ alors il existe un homomorphisme de groupe calculable vers le groupe additif $\mathbb{F}_p$, et donc le logarithme discret est de complexité polynomiale.

Il est impératif que $N \neq p$.

- Cette condition exclut les courbes supersingulières.

- Soit e le *degré de plongement*, c.-à-d. le plus petit entier tel que N divise $p^e - 1$; alors il existe un homomorphisme de groupe calculable vers le groupe multiplicatif de $\mathbb{F}_{p^e}$, et donc le logarithme discret a une complexité sous-exponentielle relativement à p^e.
  - Solution : si $e \approx p$ alors cette complexité est exponentielle relativement à p.

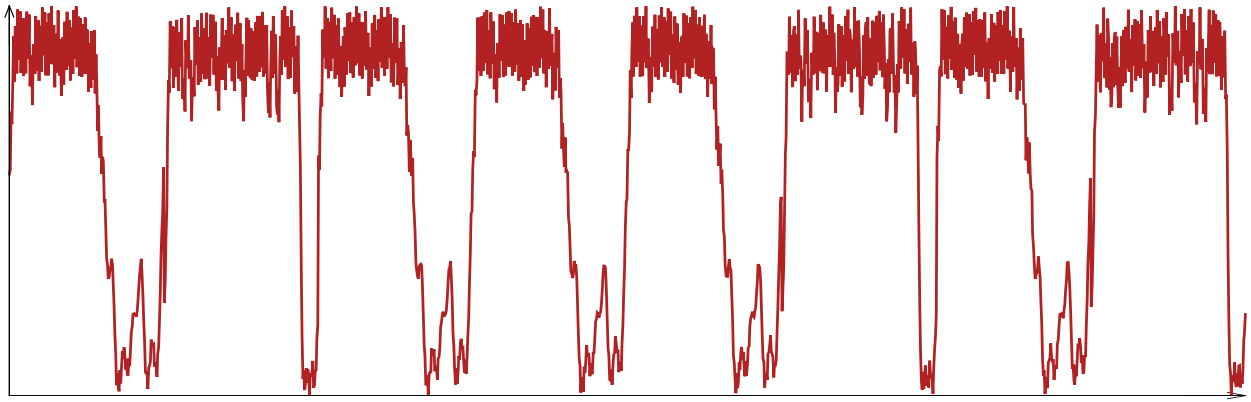
- Il est impératif que e soit assez grand ($\mathcal{P} \approx 1$).
- Pour calculer e, il faut connaître la factorisation de $q - 1$, ce qui est sous-exponentiel (c'est asymptotiquement l'étape la plus coûteuse).


Wikigallery.org - Do not use for commercial use. Do not remove this warning.
WikiGallery.Org

Résistance des implémentations de la courbe

Il existe des courbes pour lesquelles, bien que le logarithme discret soit difficile, certaines implémentations ou certains protocoles sont faibles.

Exemple : multiplication par l'algorithme « doublement et addition » non protégé.



D	A	D	D	D	A	D	A
1		0	0	1		1	

Contre-mesures classiques

- Contre les attaques simples : élimination des branches conditionnelles sur un élément secret.
  - double and always add :

$$
\begin{aligned}
&Q \longleftarrow P;\\
&\texttt{for } i = \ell - 2, \dots, 0\texttt{:}\\
&\qquad Q_0 \longleftarrow 2Q;\ Q_1 \longleftarrow Q_0 + P;\ Q \longleftarrow Q_{n_i};
\end{aligned}
$$

  - échelle de Montgomery :

$$
\begin{aligned}
&Q_0 \longleftarrow P; Q_1 \longleftarrow 2P;\\
&\texttt{for } i = \ell - 2, \dots, 0\texttt{:}\\
&\qquad Q_{1-n_i} \longleftarrow Q_0 + Q_1;\ Q_{n_i} \longleftarrow 2Q_{n_i};
\end{aligned}
$$

- Contre les attaques différentielles : ne pas manipuler plusieurs fois le même élément secret.
  - masquage aléatoire du secret ($n \leftarrow n + r \cdot N$ avec r aléatoire) ;
  - masquage aléatoire de la courbe ($a \leftarrow r^4 a, b \leftarrow r^6 b$) ;
  - masquage aléatoire du point ($(x : y : 1) \leftarrow (rx : ry : r)$)...

Petit sous-groupe

Si la courbe possède un petit sous-groupe, alors il est possible, dans certains protocoles, d'obtenir de l'information sur des données secrètes [Lim-Lee 97].

- Si le point de base G est d'ordre m, alors l'observation de aG permet de retrouver la valeur $a \pmod m$.
- Suppose un adversaire capable de fournir un point de base de son choix.

Il est préférable que le groupe des points de la courbe soit d'ordre premier ($\mathcal{P} = 1$ si N premier).

Sécurité de la courbe tordue

La *courbe tordue* de E est la courbe E' d'équation

$$dy^2 = x^3 + ax + b, \qquad \text{où } d \text{ n'est pas un carré dans } \mathbb{F}_p.$$

Pour tout $x \in \mathbb{F}_p$ tel que $x^3 + ax + b \neq 0$, il existe un point d'abscisse x sur exactement une des deux courbes E et E'.
Dans certains cas, un adversaire peut injecter une abscisse appartenant à la courbe tordue [Fouque-Lercier-Réal-Valette 2008] :

- protocole mal conçu (compression de point),
- manque de tests dans l'implémentation,
- attaque par injection de faute...

Il est préférable que la courbe tordue soit sûre.
($\mathcal{P} \approx \frac{1}{\log p}$.)

Points spéciaux

Un *point spécial* est un point de la courbe de la forme $(0, y)$ ou $(x, 0)$.
En présence de tels points, certaines implémentations peuvent faire fuir de l'information [Goubin 2003].

- Des points spéciaux de la forme $(0, y)$ existent si b est un carré dans k ($\mathcal{P} = 1/2$).
- Des points spéciaux de la forme $(x, 0)$ existent si N est pair ($\mathcal{P} = 1$ si N premier).

Il est préférable que la courbe ne contienne pas de tels points spéciaux.

- Des points spéciaux de la forme $(0, y)$ existent toujours sur la courbe ou sa tordue.
($\mathcal{P} = 1$).

Corps de base spéciaux

De nombreuses courbes standard ont des corps de base spéciaux :

$$p_{192} = 2^{192} - 2^{64} - 1$$
$$= \texttt{0xfffffffffffffffffffffffffffffffeffffffffffffffff}.$$

- Puisque $N = p + O(\sqrt{p})$, les premiers bits de N sont les premiers bits de p.
- Les premiers bits de $n + r \cdot N$ sont les premiers bits de r.
- Ceci rend la protection par masquage de n insuffisante [DK2005, BPSY2014, FRV2014, SW2015...].

Il est préférable que le corps de base ne soit pas d'une forme spéciale.

Loi de groupe unifiée

Certaines courbes admettent une loi d'addition *unifiée* : il existe un système de coordonnées permettant d'effectuer les opérations $P+Q$, $2P$, $P+0$ par les mêmes formules.

- Courbes d'Edwards : $x^2+y^2=c^2(t^2+dz^2)$, $xy=zt$;
- Courbes de Jacobi : $y^2=z^2+2ax^2+bt^2$, $x^2=zt$...

Ceci est possible sous certaines conditions sur la courbe :

- Edwards : point de 4-torsion, $\mathcal{P}=17/48$;
- Jacobi : point de 2-torsion, $\mathcal{P}=2/3$...

Ceci ajoute une couche de protection contre les attaques simples.

Résistance à de possibles attaques futures

- Et s'il existait des familles faibles ?
- Éviter de produire des courbes trop « particulières ».
- Vérifier des propriétés satisfaites avec $\mathcal{P} \approx 1$.
- En particulier, vérifier que différents nombres attachés à la courbe sont « assez grands ».

Discriminant du corps des endomorphismes

- Le *corps des endomorphismes* de E est l'extension quadratique K de $\mathbb{Q}$ engendrée par le Frobenius φ.
- Le polynôme minimal de φ est $\varphi^2 - t\varphi + p$; son discriminant est $D_\varphi = t^2 - 4p < 0$.
- Le discriminant de K est donné par $D_\varphi = D_K f_\varphi^2$, où D_K ou $D_K/4$ est sans facteur carré.

En général, $|D_K| \approx p$; en particulier, $|D_K| \geq \sqrt{p}$ avec $\mathcal{P} \approx 1 - O(1/\sqrt{p})$.

- Cette condition élimine les valeurs $D_K = -3$ et -4, correspondant aux j-invariants 0 et 1728.

Nombre de classes

Le nombre de classes h_K de K intervient dans divers algorithmes liés à E :

- c'est le degré du polynôme de Hilbert à factoriser pour la théorie de la multiplication complexe ;
- c'est le plus petit degré d'une extension $L/\mathbb{Q}$ sur laquelle E admet un relèvement fidèle.

Ce nombre est minoré en fonction de D_K :

$$h_K \geq C \frac{\sqrt{|D_K|}}{\log |D_K|}.$$

$\Rightarrow$ aucune condition supplémentaire sur h_K n'est a priori nécessaire.

Friabilité du nombre de classes

- Le nombre de classes h_K est l'ordre du groupe de classes de K.
- Pour éviter de potentielles attaques utilisant la décomposition de ce groupe en facteurs élémentaires, on souhaite que h_K ne soit pas friable (= n'ait pas que des petits facteurs premiers).
- Un nombre aléatoire n est $n^{1/u}$-friable avec probabilité $\mathcal{P} \approx u^{-u}$.
- Par conséquent, h_K a une probabilité négligeable d'être $(\log p)^{O(1)}$-friable.

En général, h_K a au moins un diviseur premier $\geq (\log p)^{O(1)}$.

- Calculer (et factoriser) h_K est sous-exponentiel [Biasse 2010], mais vérifier que h_K n'est pas logarithmiquement friable est polynomial.

Friabilité de la courbe tordue

- Si la courbe E a pour cardinal $N = p + 1 - t$, alors sa tordue E' a pour cardinal $N' = p + 1 + t$.
- Le cardinal N' est $p^{1/u}$-friable avec probabilité $\mathcal{P} \approx u^{-u}$.
  - Par exemple, N' est $p^{1/4}$-friable avec probabilité $1/256$.

En général, N' a au moins un diviseur premier de taille polynomiale en p.

- Le choix du seuil u est délicat ; par exemple, pour $p \approx 2^{256}$, une probabilité 2^{-128} correspond aux nombres 727-friables...
- Variante plus stricte de cette condition : N' premier (= courbe tordue sûre).

Corps de base spécial

- Certaines courbes utilisent des corps de base dont la cardinalité est un nombre premier « spécial » : une valeur d'un « petit » polynôme.
  - ▷ NIST $p_{192} = 2^{192} - 2^{64} - 1 = x^3 - x - 1$ où $x = 2^{64}$.
- Le logarithme discret *multiplicatif* est plus facile dans de tels corps que dans le cas général.
- Il est envisageable que des attaques analogues soient découvertes sur les courbes elliptiques.

Il est souhaitable de choisir un nombre premier pseudo-aléatoire.

- Il est impossible de vérifier si un nombre est une valeur d'un « petit » polynôme...

Degré de plongement

- Le degré de plongement est l'ordre de p dans le groupe multiplicatif $\mathbb{F}_q^\times$.

Le degré de plongement est $\geq p^{1/4}$ avec probabilité $\mathcal{P} \geq 1 - 1/\sqrt{p}$.

Structure multiplicative du corps de base

- La structure multiplicative de $\mathbb{F}_p^\times$ dépend de la factorisation de $p-1$.
- Même si elle n'est pas liée au logarithme discret sur une courbe, en général $p-1$ a au moins un grand diviseur premier.

$p-1$ a un diviseur premier $\geq (\log p)^2$ avec probabilité $\geq 1 - 1/\sqrt{p}$.

Résumé

	NIST	Brainpool	ANSSI	OSCCA
N premier	✓	✓	✓	✓
p ordinaire		✓	✓	✓
Loi unifiée				
N' premier				
Générique		✓	✓	✓
	NUMS	Curve25519/41417	Ed448-Goldilocks	
N premier				
p ordinaire				
Loi unifiée	✓	✓	✓	
N' premier	✓	✓	✓	
Générique				

Facilitation de l'implémentation

Certains choix de courbes permettent de disposer d'implémentations plus rapides ou plus commodes.

Coordonnées jacobiennes rapides

Une courbe elliptique de la forme $y^2 = x^3 - 3x + b$ (c'est-à-dire telle que $a = -3$) permet d'économiser 2 des 10 multiplications requises pour une addition de points.

Une courbe aléatoire sur $\mathbb{F}_p$ est isomorphe avec une courbe $a = -3$ avec probabilité

- $\mathcal{P} = 1/4$ si $p \equiv +1 \pmod 4$,
- $\mathcal{P} = 1/2$ si $p \equiv -1 \pmod 4$.

Nombre de points

Si la courbe a $N < p$ points, alors un élément de $\mathbb{Z}/N\mathbb{Z}$ peut être représenté par un nombre de la même taille que p.

Exactement la moitié des courbes satisfont cette condition.

Racines carrées rapides

Si $p \equiv -1 \pmod 4$ (ou $p \equiv 5 \pmod 8$) alors calculer des racines carrées modulo p est plus facile, ce qui permet de simplifier la compression de points.

Arithmétique dédiée

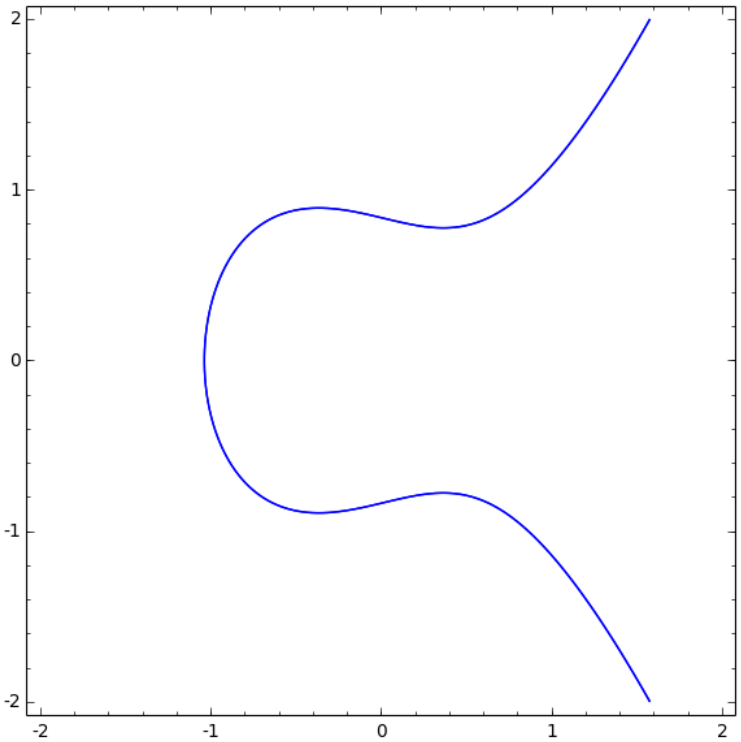
- Certains choix de corps de base, comme les nombres premiers « spéciaux » des courbes NIST, permettent une arithmétique plus rapide.
- De même, choisir des petites valeurs pour les paramètres a et b permet d'accélérer l'arithmétique de la courbe.

Différents critères pour différents usages

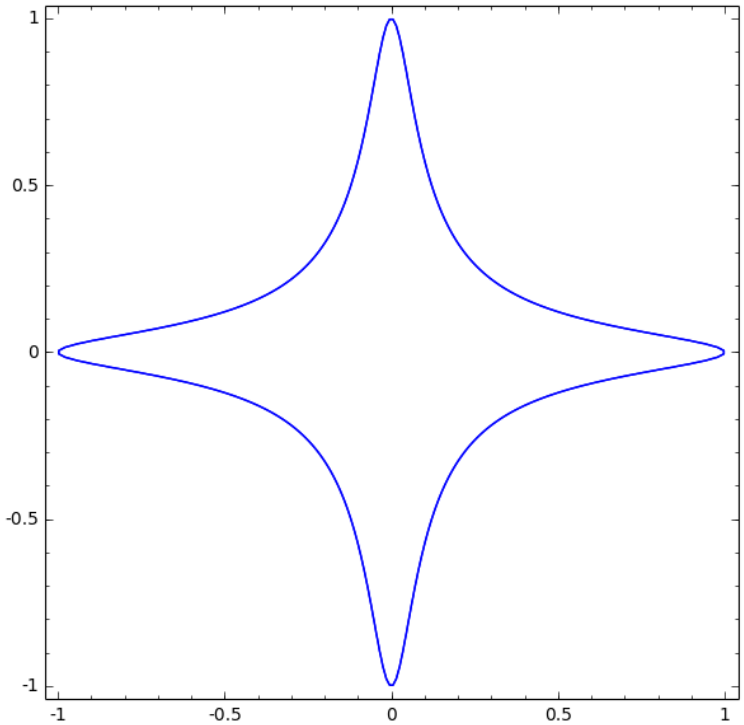
- Les critères précédemment énoncés ne peuvent être tous vérifiés.
- En particulier, compromis vitesse/généricité.
- Mais aussi, facilité d'implémentation/protection latérale.

Il est souhaitable d'utiliser (et de normaliser) différentes courbes pour différents usages !

Modèles réels

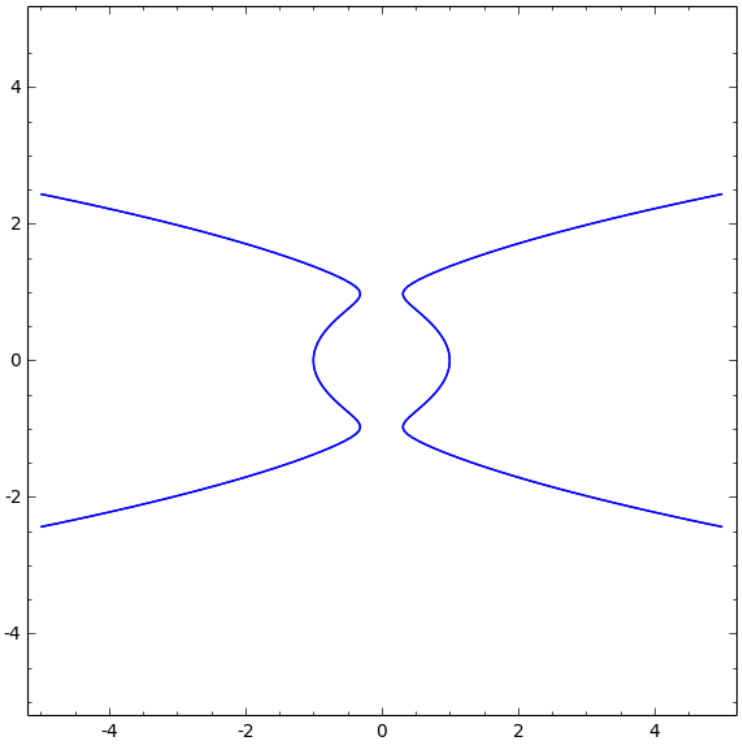


Weierstrass

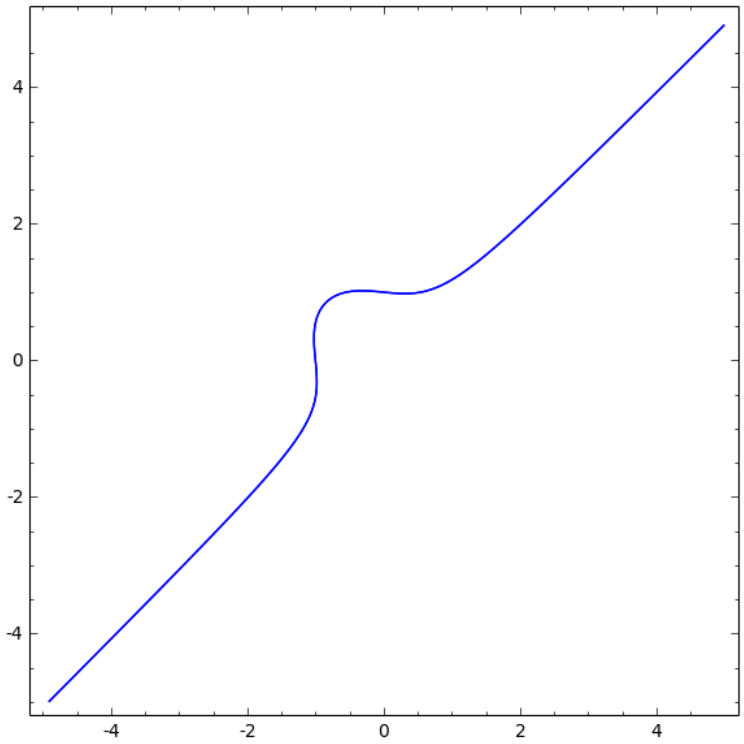


Edwards

Modèles réels (II)

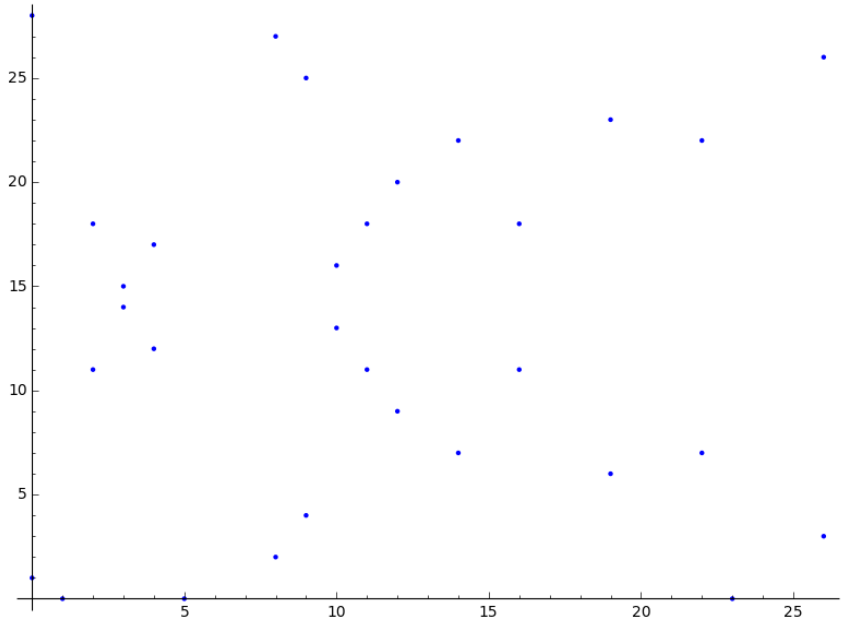


Jacobi

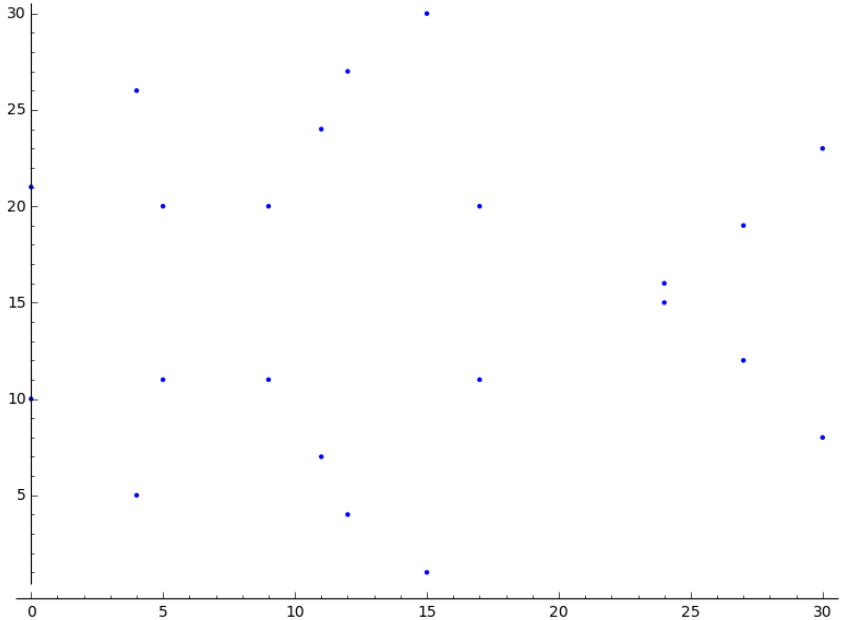


Hess

Modèles finis

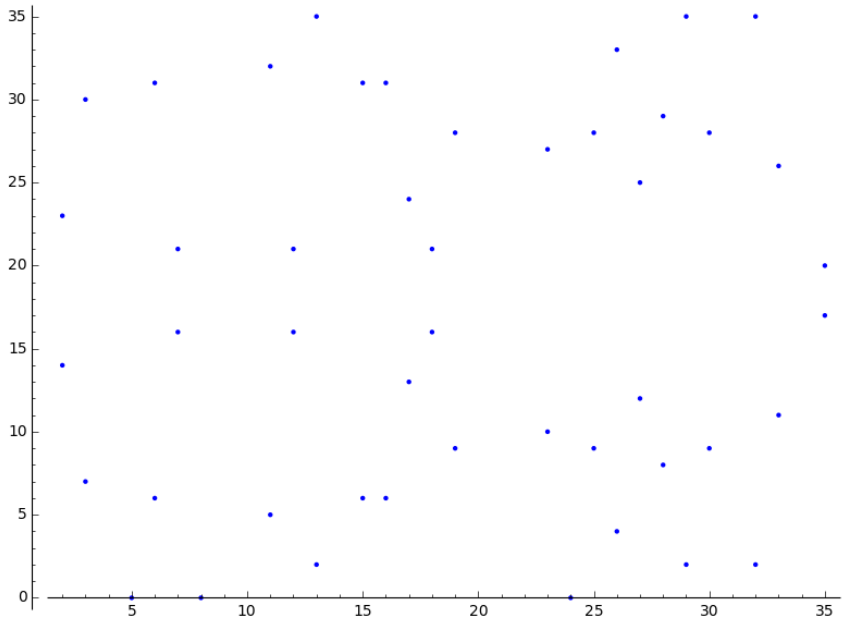


Grenouille

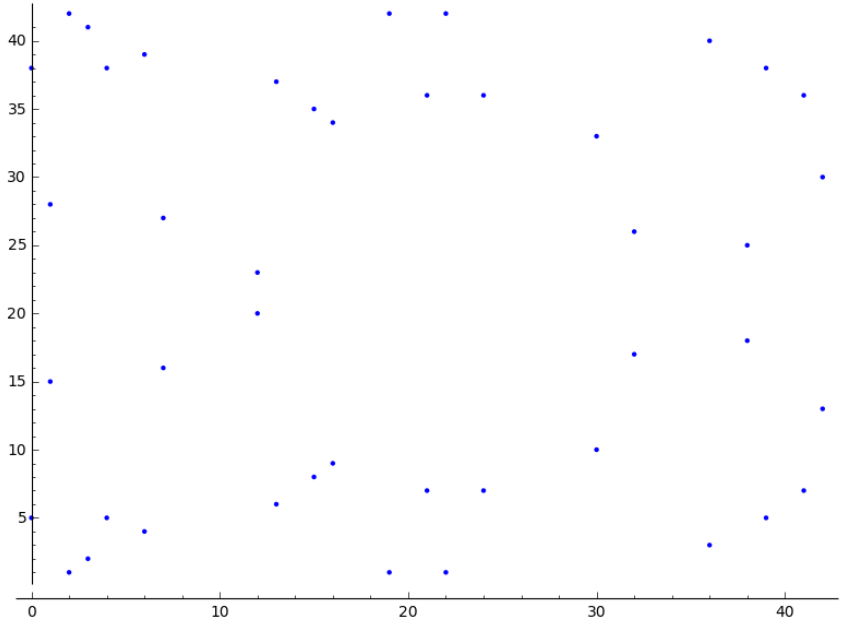


Cafard

Modèles finis (II)



Morse



Lapin

III – Transparence

Transparence

Architecture

- Fournir des courbes remplissant les conditions ci-dessus...
- ... accompagnées d'un **certificat** permettant de vérifier les propriétés sans refaire tous les calculs :
  - nombre de points,
  - discriminant et nombre de classes,
  - degré de plongement.

- Programme **déterministe** pour échantillonner une courbe.
  - Processus de génération entièrement reproductible.
  - Peut être un générateur pseudo-aléatoire (généricité) ou une énumération des petites valeurs (efficacité).
  - Certifier toutes les étapes du processus, y compris les courbes rejetées.

Nombre de points premier

- On connaît la borne de Hasse-Weil : $|N - (p+1)| \leq 2\sqrt{p}$.
- Si $G \neq 0$ est tel que $q \cdot G = 0$ avec $q \geq p - 2\sqrt{p} + 1$ premier, alors $q = N$.
- Certificat de primalité de N : (G, q, Π), où Π est une preuve de primalité de q.
  - Pour les tailles usuelles de courbes elliptiques, Π peut être laissée vide ; en effet, pour ces tailles, une preuve directe par APR-CL est probablement plus rapide qu'une preuve par certificat ECPP.
- Ce certificat est produit une seule fois, pour la courbe finale.
- Taille du certificat et vérification en $O(\log^2 p)$ opérations.

Nombre de points composé

- Si $n < 2(\sqrt{p}-1)^2$ est composé et si $P \neq 0$, $n \cdot P = 0$, alors l'ordre de la courbe est composé.
  - preuve : soit $d = \gcd(n, N)$; alors $d \neq 1$ car $P \neq 0$. Si $d \neq N$ alors d est un diviseur strict de N. Si $d = N$ alors N divise n ; puisque $n/2 < (\sqrt{p}-1)^2$, on a nécessairement $N = n$, qui est composé.
- Certificat de composition de N : (n, c, P), où c est un témoin de composition (Miller-Rabin) de n.
- Complexité pour chacune des $O(\log p)$ ou $O(\log^2 p)$ courbes :
  - production du certificat : $O(\log p)$ multiplications ;
  - taille du certificat : $O(\log p)$;
  - vérification : $O(\log p)$ multiplications.

Nombre de points composé (II)

- En pratique, le calcul du nombre de points N se fait en calculant $N \pmod{\ell}$ pour de petits nombres premiers ℓ.
- Si on trouve $N \equiv 0 \pmod{\ell}$, on peut arrêter le calcul pour cette courbe !

- Dans ce cas, on trouve un polynôme f_ℓ, de degré $O(\ell)$, dont les racines sont les abscisses de points de ℓ-torsion.
- Trouver une racine de ce polynôme (par Cantor-Zassenhaus) a un coût comparable à celui du calcul de $N \pmod{\ell}$.
- Dans ce cas, (ℓ, P) est un certificat de composition.

Discriminant et nombre de classes

- Le calcul du discriminant nécessite de factoriser le nombre $D_\varphi = t^2 - 4p$.
- C'est asymptotiquement l'une des étapes dominantes du processus de génération de la courbe ($L(1/3)$).
- Certificat : la factorisation de D_φ.

- Le calcul exact du nombre de classes est probablement hors de portée ($L(1/2)$).
- Il suffit d'un élément pour prouver que le nombre de classes est grand.
- Il est impossible de prouver réalistement que la courbe a été rejetée pour cause de nombre de classes trop petit.
  - ▷ Solution : générer quelques éléments (déterministes) du groupe de classes et prouver que l'on ne peut pas prouver avec ces éléments que le nombre de classes est assez grand.

Exemple

- Fonction d'échantillonnage pour une graine s :
  - $p =$ le plus petit premier $\geq s$;
  - $g =$ le plus petit générateur de $\mathbb{F}_p^\times$;
  - courbes de la forme $y^2 = x^3 - 3x + b$, $b = g, g^2, \ldots$.
- Conditions :
  - N et N' premiers ;
  - $\Delta \neq 0$, $N, N' \neq p, p+1$;
  - degré de plongement de E, E' au moins $p^{1/4}$;
  - nombre de classes $\geq p^{1/4}$.

Exemple de certificat

Pour la graine $s = 2015$: $p = 2017$, $g = 5$,

Curve

```
(2017, -3, 625)
order = 2063, point = (0, 25)
twist_order = 1973
disc_factors = {6043}
class_number = 9, form = (17,3,89)
embedding_degree = 1031, factors = {2, 1031}
twist_embedding_degree = 493, factors = {2, 17, 29}
```

Rejected curves

```
((2017, -3, 5), composite, 2065, witness, 1679, point, (1,258))
((2017, -3, 25), torsion_point, 3, point, (448, 288))
((2017, -3, 125), torsion_point, 2, point, (982, 0))
```

Non-manipulabilité

- Ce processus permet de produire **déterministement** une courbe elliptique cryptographique à partir
  - d'un ensemble de conditions (y compris bornes numériques),
  - d'une fonction d'échantillonnage des courbes (y compris graine éventuelle).
- Seules quelques conditions influenceront probablement le résultat final :
  - sécurité de la courbe tordue,
  - choix des bornes de friabilité.
- Pour éviter tout soupçon sur le choix de la graine :
  - utiliser un schéma d'engagement sur des fragments de la graine ;
  - utiliser un résultat hors de portée de manipulation (cours de la Bourse, résultat sportif, loterie publique).

Graine

Questions ?