Filières MP/MPI - ENS de Paris-Saclay, Lyon, Rennes et Paris - Session 2026
Page de garde du rapport de TIPE

Attention: Le rapport doit être réalisé par l'étudiant(e).
Si le rapport résulte d'une collaboration, elle doit être clairement annoncée.

NOM : GOUDEV	Prénoms : Antoine, Gilles, Maxime
Classe : MP*	
Lycée : Louis-Le-Grand	Numéro de candidat : 32037
Ville : Paris	

Concours auxquels vous êtes admissible (les indiquer par une croix) :

Banque MP

ENS Paris-Saclay	MP - Option MP	X
	MP - Option MI	
ENS de Lyon	Math - Option M-MP	
	Math - Option M-MI	
	Informatique	X
ENS Rennes	MP - Option MP	
	MP - Option MI	X
ENS Paris	MP - Option P	
	MP - Option I	X

Banque MPI

ENS Paris-Saclay	Option Math	
	Option Info	
ENS de Lyon	Math MPI	
	Info MPI	
ENS Rennes	Info MPI	
ENS Paris	Option Math	
	Option Info	

Matière dominante du TIPE (la sélectionner d'une croix inscrite dans la case correspondante) :

Informatique	X	Mathématiques		Physique	

Titre du TIPE : Courbes elliptiques et cryptographie

Nombre de pages (à indiquer dans les cases ci-dessous) :

Texte	5	Illustration	1	Bibliographie	1

Attention, les illustrations doivent figurer dans le corps du texte et non en fin du document !

Résumé ou descriptif succinct du TIPE (6 lignes, maximum) :

Grâce aux courbes elliptiques, la cryptographie moderne dispose de chiffrements efficaces. À l'issue d'un travail théorique sur la structure des courbes elliptiques, nous analyserons plusieurs chiffrements asymétriques. Cette approche est concrétisée par une implémentation Python qui permet d'éprouver ces protocoles face à différentes attaques

À Paris

Le 30/05/2026

Signature du (de la) candidat(e) AG

Signature du professeur responsable de la classe préparatoire dans la discipline

Cachet de l'établissement

Lycée Louis le Grand
075 0655 E
123, rue St Jacques
75231 PARIS CEDEX 05
Tél. 01 44 32 82 00

La signature du professeur responsable et le tampon de l'établissement ne sont pas indispensables pour les candidats libres (hors CPGE).

Courbes elliptiques et cryptographie

Antoine Goudey
Rapport de TIPE

2026

1 Introduction

À chaque nouvelle conversation, WhatsApp affiche que nos messages sont « chiffrés de bout en bout ». Mais au-delà du slogan marketing, peut-on avoir la certitude mathématique que nos échanges sont indéchiffrables ? Et si le calcul pour les sécuriser est si complexe, comment se fait-il que l'envoi soit instantané depuis un simple smartphone ?

L'application utilise le Protocole Signal (et son algorithme d'échange de clés X25519), dont l'exécution repose sur les courbes elliptiques. Dans quelle mesure la structure de groupe des courbes elliptiques permet-elle d'optimiser le ratio sécurité/performance par rapport à d'autres cryptosystèmes, et quelles sont les limites concrètes de cette robustesse face à différentes attaques ?

2 Définitions : des courbes elliptiques à la loi de groupe

2.1 Une courbe elliptique

Définition 2.1. Dans le cadre de ce TIPE, une courbe elliptique sera définie comme l'ensemble des solutions de l'équation $y^2 = x^3 + ax + b$, avec $4a^3 + 27b^2 \neq 0$ sur un corps $K = \mathbb{F}_p$, auxquelles on ajoute un point à l'infini ∞.

Définition 2.2. Si $P(x, y) \in E$, on définit $-P = (x, -y)$, et $-P = \infty$ si $P = \infty$.

2.2 Addition de points

Définition 2.3. Algébriquement, on a :

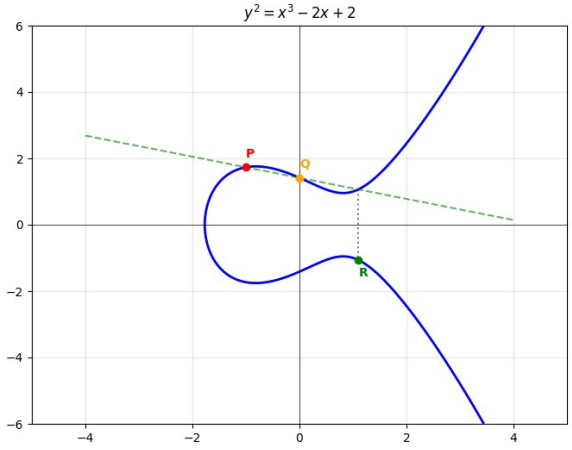
- $P + \infty = \infty + P = P$
- $P + (-P) = \infty$
- Si $P = (x_p, y_p)$, $Q = (x_q, y_q)$ et $Q \neq \pm P$, on pose $P + Q = S(x_s, y_s)$, avec :

$$\begin{cases} x_s = \left(\frac{y_q - y_p}{x_q - x_p}\right)^2 - x_p - x_q \\ y_s = \left(\frac{y_q - y_p}{x_q - x_p}\right)(x_p - x_s) - y_p \end{cases}$$

- Si $P(x_p, y_p)$, et $P \neq -P$, alors $P + P = S(x_s, y_s)$, avec :

$$\begin{cases} x_s = \left(\frac{3x_p^2 + a}{2y_p}\right)^2 - 2x_p \\ y_s = \left(\frac{3x_p^2 + a}{2y_p}\right)(x_p - x_s) - y_p \end{cases}$$

Remarque 2.1. Géométriquement, sur $\mathbb{R}$, c'est la méthode "cordes et tangentes"



2.3 Structure de groupe

L'ensemble des points $E(K)$ muni de cette loi d'addition forme un **groupe abélien**.

Théorème 2.1. (Hasse, 1924) Soit $N = \text{Card}(E(\mathbb{F}_p))$

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

Corollaire 2.1. N est proche de $p+1$, et en particulier, $N \geq p + 1 - 2\sqrt{p}$.

Ce corollaire est très important car il assure que si p est "grand", les courbes elliptiques sur $\mathbb{F}_p$ ont un ordre élevé (ce qui est nécessaire pour que la courbe soit sûre).

Théorème 2.2. Théorème de structure des courbes elliptiques Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$. Alors il existe des entiers m_1, m_2 tels que :

$$E(\mathbb{F}_q) \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

avec $m_1 | m_2$. [1]

3 Utilisation en cryptographie

3.1 Le problème du logarithme discret elliptique

Définition 3.1. Étant donné une courbe $E(\mathbb{F}_p)$, un point $P \in E$ d'ordre ω, et un point $Q \in \langle P \rangle$, le problème du logarithme discret consiste à trouver l'unique entier $n \in \{0, 1, \ldots, \omega - 1\}$ tel que $Q = nP$.

Hypothèse. Le problème du logarithme discret est un problème "difficile" : il n'existe pas à l'heure actuelle d'algorithme classique (non quantique) de résolution avec une complexité polynomiale en le nombre de bits de ω.

3.2 Méthode de Koblitz [2]

L'objectif est de transformer un message $m \in \mathbb{N}$ en un point de la courbe, que l'on pourra ensuite chiffrer. On se place sur une courbe $E(\mathbb{F}_p)$, et on se donne un entier K (typiquement $K = 100$). Pour pouvoir appliquer l'algorithme, il faut satisfaire la condition :

$$(m+1)K < p$$

1. Hankerson et al., 2004.
2. Koblitz, 1987.

Pour $j = 1, 2, \ldots$, on teste si $x = mK + j$ est tel que $x^3 + ax + b$ est un résidu quadratique modulo p. Si c'est le cas, alors on peut trouver y tel que (x, y) est un point de la courbe, et on associe à m le point (x, y). Sinon, on continue. Puisqu'il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$, la probabilité d'échec est d'environ $\frac{1}{2}$ à chaque étape. Pour $K = 100$, c'est négligeable.

3.3 Chiffrement d'El Gamal sur courbes elliptiques [3] [4]

3.3.1 Création d'une paire de clés

Les paramètres fournis sont une courbe $E(\mathbb{F}_p)$, un point P d'ordre ω (définis par exemple dans le protocole) Pour créer une paire de clés, on tire un entier aléatoire $d \in \{1, 2, \ldots, \omega - 1\}$, et on calcule $Q = dP$

— La clé publique est Q (et (P, ω), déterminés au moment du choix de la courbe)
— La clé privée est d

3.3.2 Chiffrement d'un message

Supposons que le message soit $M \in E$ (transformé d'un entier en un point par Koblitz). Pour chiffrer un message, il faut choisir un entier aléatoire $k \in \{1, 2, \ldots, \omega - 1\}$. Le message chiffré est :

$$(C_1, C_2) = (kP, M + kQ)$$

Pour récupérer M, le destinataire utilise sa clé privée d pour calculer $dC_1 = dkP = kQ$, puis $M = C_2 - kQ$.

Pour trouver M, un attaquant doit trouver kQ, ce qui revient à résoudre le problème du logarithme discret car $kQ = dC_1$.

3.4 Protocole d'échange de clés de Diffie-Hellman [5]

En pratique, le cryptosystème d'ElGamal n'est pas utilisé à cause de la condition d'utilisation de Koblitz, qui impose que la taille des messages ne soit pas trop grande. Pour p premier de 256 bits, m est inférieur à $2^{256}/K$, on peut chiffrer moins de 32 octets par point. On utilise plutôt le protocole d'échange de clé de Diffie-Hellman sur les courbes elliptiques. Ce dernier permet à deux entités (ici, Alice et Bob), de convenir d'un secret partagé en communiquant sur un canal non sécurisé. Ce protocole repose sur la connaissance publique des paramètres de la courbe elliptique, et notamment d'un point générateur G. Le processus se déroule de manière parfaitement symétrique et simultanée.

1. Indépendamment l'un de l'autre, Alice et Bob tirent au hasard un entier qui constituera leur clé privée : n_A et n_B. Chacun calcule ensuite son point public : Alice calcule $P_A = n_A G$, et Bob calcule $P_B = n_B G$.
2. Alice transmet P_A à Bob, tandis que Bob transmet P_B à Alice. Un éventuel attaquant interceptant cette communication ne verrait passer que les points P_A et P_B. Retrouver n_A ou n_B à partir de ces points équivaudrait à résoudre le problème du logarithme discret elliptique.
3. Alice multiplie la clé publique de Bob par sa propre clé privée pour obtenir le point $S = n_A P_B$. Bob procède de même pour obtenir le point $S = n_B P_A$. L'associativité de l'addition assure l'égalité des deux points obtenus.

3. ElGamal, 1985.
4. Hoffstein et al., 2010.
5. Diffie et Hellman, 1976.

4 Attaques et résultats expérimentaux

4.1 Attaque de Pollard's rho [6]

4.1.1 Algorithme

Théorème 4.1. Cycle de Floyd Soit $f : I \to I$ une fonction, avec I un ensemble fini. Soit $a_0 \in S, a_{n+1} = f(a_n)$. Alors la suite (a_n) est périodique à partir d'un certain rang n_0, de période k. De plus, il existe m tel que $a_m = a_{2m}$, et $n_0 \leq m < n_0 + k$.

Démonstration. Comme I est fini, il existe $n_1 < n_2$ tels que $a_{n_1} = a_{n_2}$. Soit n_0 le plus petit entier tel que a_{n_0} soit égal à un terme suivant dans la suite. Alors $a_{n_0} = a_{n_0+k}$ pour un certain $k > 0$. Si $i > 0$, $a_{n_0+i} = f(f(f(\dots f(a_{n_0})))) = f(f(f(\dots f(a_{n_0+k})))) = a_{n_0+i+k}$. Donc la suite est k-périodique à partir de n_0. De plus, si l'on considère $n_0, n_0+1, \dots, n_0+k-1$, un de ces entiers est congru à 0 modulo k. Soit m cet entier. On a $2m \equiv m \pmod{k}$. Donc $a_m = a_{2m}$, et $n_0 \leq m < n_0 + k$ □

Ce théorème permet d'effectuer une attaque avec une mémoire constante.

- On part d'un point $a_0 = c_0 P + d_0 Q \in \langle P \rangle$
- On dispose d'une fonction f "aléatoire" qui, à partir de $a_n \in \langle P \rangle$, calcule $a_{n+1} \in \langle P \rangle$, et les coefficients c_{n+1} et d_{n+1} tels que $a_{n+1} = c_{n+1}P + d_{n+1}Q$.
- On calcule a_m et a_{2m} jusqu'à trouver $a_m = a_{2m}$. Cela donne $c_m P + d_m Q = c_{2m} P + d_{2m} Q$, donc $(c_m - c_{2m})P = (d_{2m} - d_m)Q$
- Enfin : $n \equiv (c_m - c_{2m}) \times (d_{2m} - d_m)^{-1} \pmod{\omega(P)}$

Remarque 4.1. En pratique, la fonction f n'est pas véritablement aléatoire (f doit être déterministe pour être sûr d'avoir un cycle), mais on veut utiliser une fonction peu régulière et non injective pour que l'algorithme ne soit pas une simple recherche exhaustive. Pour mes simulations, j'ai utilisé la fonction suivante (choisie heuristiquement) :

$$f : R \in \langle P \rangle \mapsto \begin{cases} R + P & \text{si } x_R \equiv 0 \pmod 3 \\ 2R & \text{si } x_R \equiv 1 \pmod 3 \\ R + Q & \text{si } x_R \equiv 2 \pmod 3 \end{cases}$$

Remarque 4.2. Pour pouvoir terminer l'attaque, il faut que $d_{2m} - d_m$ soit inversible modulo $\omega(P)$, et en particulier non nul. En pratique, $\omega(P)$ est premier, et la probabilité que $d_{2m} = d_m$ est de l'ordre de $\frac{1}{\omega}$, ce qui est négligeable. Cela a tout de même été source de difficultés dans mon implémentation personnelle (avec $\omega \sim 10^3$).

4.1.2 Complexité et paradoxe des anniversaires

Question. Quel est le temps d'attente moyen avant de trouver une collision ?

Cette problématique est reliée au paradoxe des anniversaires. En effet, nous cherchons deux points égaux dans le sous-groupe $\langle P \rangle$, mais avec des coefficients différents, peu importe ces points.

Théorème 4.2. Soient ω boules numérotées dans une urne. On tire les boules indépendamment et uniformément, avec remise. Soit T le nombre de tirages nécessaires pour obtenir une boule déjà tirée.

$$\mathbb{E}(T) \underset{k \to +\infty}{\sim} \sqrt{\frac{\pi\omega}{2}}$$

$$\sigma(T) \underset{k \to +\infty}{\sim} \sqrt{\left(2 - \frac{\pi}{2}\right)\omega}$$

6. Hankerson et al., 2004.

L'attaque de Pollard's Rho trouve n en $O(\sqrt{\omega(P)})$ opérations, avec une mémoire constante. C'est le meilleur algorithme connu dans le cas général. Pour une courbe sécurisée sur $\mathbb{F}_p$, $\omega(P) \approx p$, car on choisit un point P tel que $\omega(P) \approx N$, et $N \approx p$ par Hasse.

4.1.3 Résultats expérimentaux

Pour obtenir les graphiques ci-dessous, j'ai généré des points aléatoires générateurs de la courbe $y^2 = x^3 + 1$, avec $p \equiv 2 \pmod 3$ premier aléatoire également. Chaque point bleu est la moyenne de 10 essais de Pollard's rho avec des points initiaux a_0 différents. Sur la figure 1, on observe un nuage de points qui suit la courbe théorique, mais les points sont très dispersés. Pour la figure 2, on génère les mêmes points, et cette fois-ci, on moyenne par tranche. Cela permet de lisser les variations aléatoires, et l'échelle log fait apparaître une droite très proche de la prévision théorique.

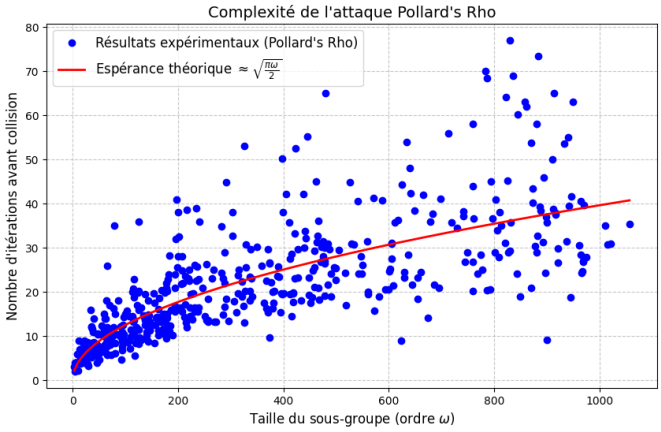


Figure 1 – Résultats bruts du nombre d'itérations de l'algorithme en fonction de la taille du sous-groupe

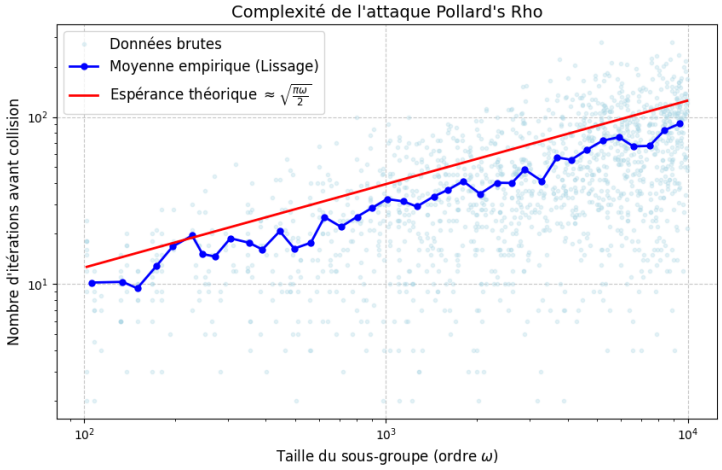


Figure 2 – Résultats lissés du nombre d'itérations de l'algorithme en fonction de la taille du sous-groupe

4.2 Attaque de Pohlig-Hellman

Toutefois, si l'ordre de la courbe est friable (divisible par des petits nombres premiers), il est possible d'améliorer significativement l'attaque de Pollard's rho, en utilisant une méthode "diviser pour régner".

- Soit $P \in E$ d'ordre ω, $Q = nP$. Supposons que $\omega = \prod_{i=1}^{k} p_i^{\alpha_i}$, avec p_i premiers.
- Soit $\omega_i = p_i^{\alpha_i}$, $P_i = \frac{\omega}{\omega_i} P$, $Q_i = \frac{\omega}{\omega_i} Q$ (P_i d'ordre ω_i).
- On résout le problème du logarithme discret sur Q_i et P_i (avec Pollard's Rho), on trouve n_i, tel que $Q_i = n_i P_i$.
- Si $n = k\omega_i + r$, $nP_i = (k\omega_i + r)P_i = rP_i$ et $nP_i = n\frac{\omega}{\omega_i} P = \frac{\omega}{\omega_i} Q = Q_i = n_i P_i$.
- Donc : $r_i \equiv n_i \pmod{\omega_i}$
- On trouve n avec le théorème des restes chinois.

La complexité de l'attaque de Pohlig-Hellman est $O(\sum_{i=1}^{r} \sqrt{p_i^{e_i}} + (\log N)^2)$, où $N = \prod_{i=1}^{r} p_i^{e_i}$ est la factorisation de l'ordre de la courbe.

4.3 Attaque par courbe invalide

Remarque 4.3. Les opérations d'addition et de doublement de points sur la courbe $(E) : y^2 = x^3 + ax + b$ ne font pas intervenir le paramètre b.

Il est donc possible pour un attaquant de choisir une courbe (E') qui possède le même paramètre a et un ordre divisible par un petit h. Il lui suffit ensuite de trouver un point d'ordre h sur cette courbe, et de l'envoyer. La victime calcule nP dans (E), mais aussi dans (E'). En testant les valeurs possibles pour kP, avec $0 \leq k < h$ (ce qui est possible car h est petit), et en comparant avec la valeur renvoyée, l'attaquant connaît. $n \pmod{h}$. Il est possible de retrouver n par le théorème des restes chinois, en itérant pour plusieurs h.

5 Conclusion

Ainsi, la cryptographie sur les courbes elliptiques est très performante, et est donc de plus en plus utilisée aujourd'hui. Malgré l'attaque de Pohlig-Hellman (si la courbe est mal choisie), et l'attaque par courbe invalide (si le protocole est mal implémenté), la meilleure attaque connue dans le cas général reste l'attaque de Pollard's rho, avec une complexité exponentielle. Toutefois, les techniques de chiffrement elliptiques sont amenées à évoluer dans le futur, puisque les ordinateurs quantiques pourront résoudre le problème du logarithme discret elliptique avec une complexité polynomiale en utilisant l'algorithme de Shor.

Références bibliographiques

ANSSI. (2026, mars). *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* (rapp. tech.). Agence nationale de la sécurité des systèmes d'information.

Aumasson, J.-P. (2017). *Serious Cryptography*. No Starch Press.

Barker, E. (2020, avril). *Recommendation for Key Management : Part 1 – General* (rapp. tech. N° NIST Special Publication (SP) 800-57 Part 1 Revision 5). National Institute of Standards et Technology.

Bernstein, D. J., & Lange, T. (2017). *SafeCurves : choosing safe curves for elliptic-curve cryptography* [Consulté le : 21/10/2025]. url.

Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, *22*(6).

ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, *31*(4).

Hankerson, D., Menezes, A., & Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography*. Springer.

Hoffstein, J., Pipher, J., & Silverman, J. (2010). *An Introduction to Mathematical Cryptography*. Springer.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), 203-209.