Mise en place d'un cryptosystème d'ElGamal sur les courbes elliptiques et étude de sa sécurité.

TIPE

February 12, 2026

Sommaire

Les courbes elliptiques

Une courbe elliptiques est l'ensemble des points de coordonnées (x, y) vérifiant l'équation :

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

où $a, b, c, d, e, f, g, h, i, j \in \mathbb{R}$ et $x, y \in \mathbb{K}$ où $\mathbb{K}$ est un corps.

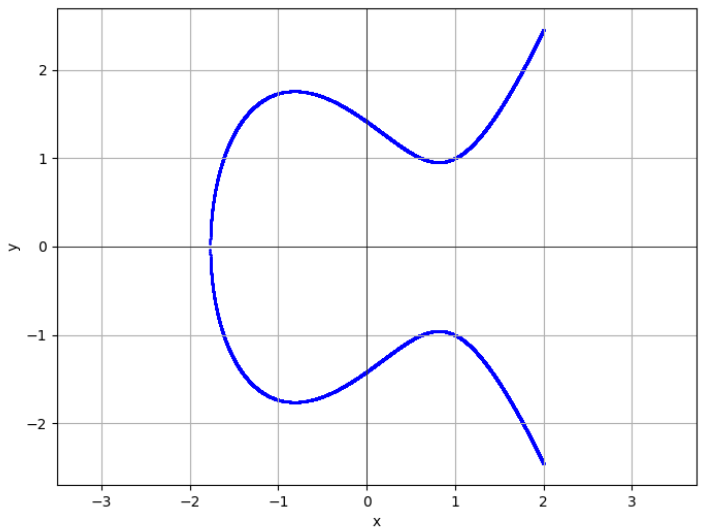


Figure: Courbe elliptique $y^2 = x^3 - 2x + 2$.

Plan projectif et point à l'infini

Definition

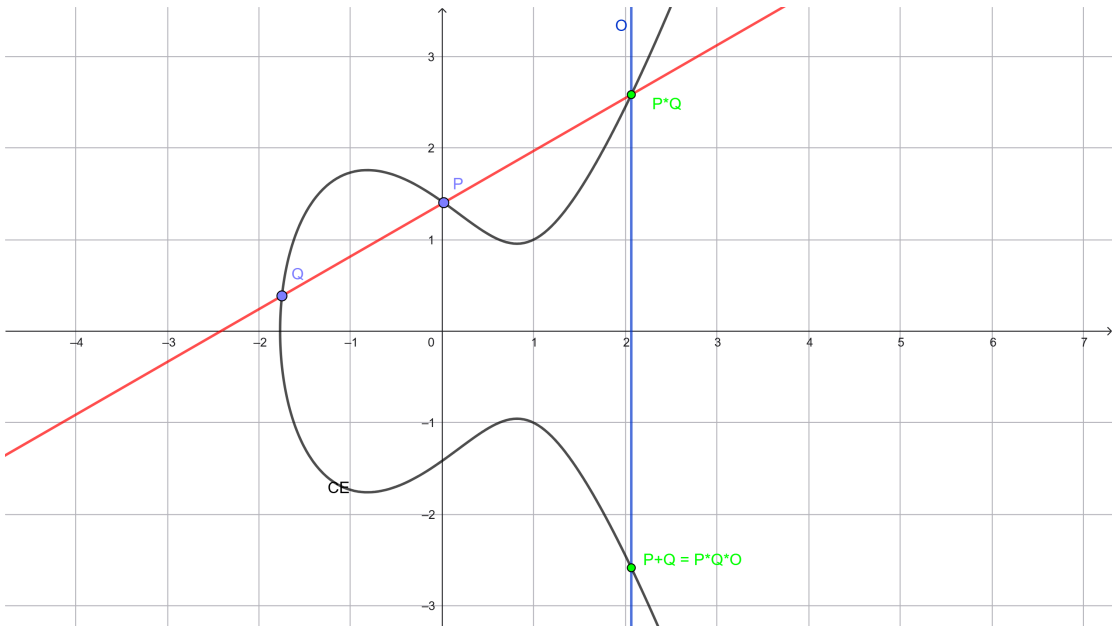
Le plan projectif $\mathbb{P}^2$ est l'ensemble des triplets de coordonnées homogènes (x, y, z) où $(x, y, z) \in \mathbb{K}^3 \setminus \{(0, 0, 0)\}$.

Definition

Dans cette notation, les points admettant des coordonnées de la forme $(x, y, 0)$ forment la droite à l'infini. Nous allons associer à la droite à l'infini un point particulier, appelé point à l'infini.

Construction de la loi de groupe

Nous allons définir une loi de groupe additive géométriquement sur les points d'une courbe elliptique.



Cette loi de group est définie de la mainière suivante :

- $P * Q = R$ où R est le troisième point d'intersection de la droit (PQ) avec la courbe elliptique.
- $P + Q = P * Q * O$ où O est le point à l'infini.

Formalisation des propriétés géométriques

Forme de Weierstrass

Les équation des courbes elliptiques définies sur $\mathbb{R}$ (ou $\mathbb{Q}$) peuvent s'écrire sous la forme :

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

où $a, b \in \mathbb{R}$ (ou $\mathbb{Q}$).

Pour P = (x_1, y_1) et Q = (x_2, y_2), en étudiant des égalités de polynômes, on obtient les formules suivantes :

P*Q = (x_3, y_3) avec : $\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$

où $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$ et $\nu = y_1 - \lambda x_1$

Construiction d'un groupe cyclique

Definition

Un groupe cyclique est un groupe à la fois monogène et fini. Il existe un élément g du groupe tel que tous les éléments du groupe soient un multipel de g.

Pour tout groupe cyclique $\mathbb{G}$ il existe $n \in \mathbb{N}$ tel que $\mathbb{G}\ \mathbb{Z}/n\mathbb{Z}$.

Application aux courbes elliptiques

Pour chaque couple d'entiers (x, y) vérifiant l'équation de la courbe elliptique, on applique un modulo à x et à y. L'équation de la courbe devient donc :

$$y^2 = x^3 + ax + b \mod n$$

ElGamal

Logarithme discret

Attaque par force brute

Algorithme du rho de Pollard

Equation

$$\cos^3\theta = \frac{1}{4}\cos\theta + \frac{3}{4}\cos 3\theta \tag{1}$$

Verbatim

Example (Theorem Slide Code)

```
\begin{frame}
 \frametitle{Theorem}
 \begin{theorem}[Mass--energy equivalence]
  $E = mc^2$
 \end{theorem}
\end{frame}
```

Slide without title.

Citing References

An example of the `\cite` command to cite within the presentation:

This statement requires citation [Smith, 2022, Kennedy, 2023].

References


John Smith (2022)
Publication title
Journal Name 12(3), 45 – 678.


Annabelle Kennedy (2023)
Publication title
Journal Name 12(3), 45 – 678.

Acknowledgements

Smith Lab

- Alice Smith
- Devon Brown

Cook Lab

- Margaret
- Jennifer
- Yuan

Funding

- British Royal Navy
- Norwegian Government

The End

Questions? Comments?