Les maths au secours des transactions bancaires

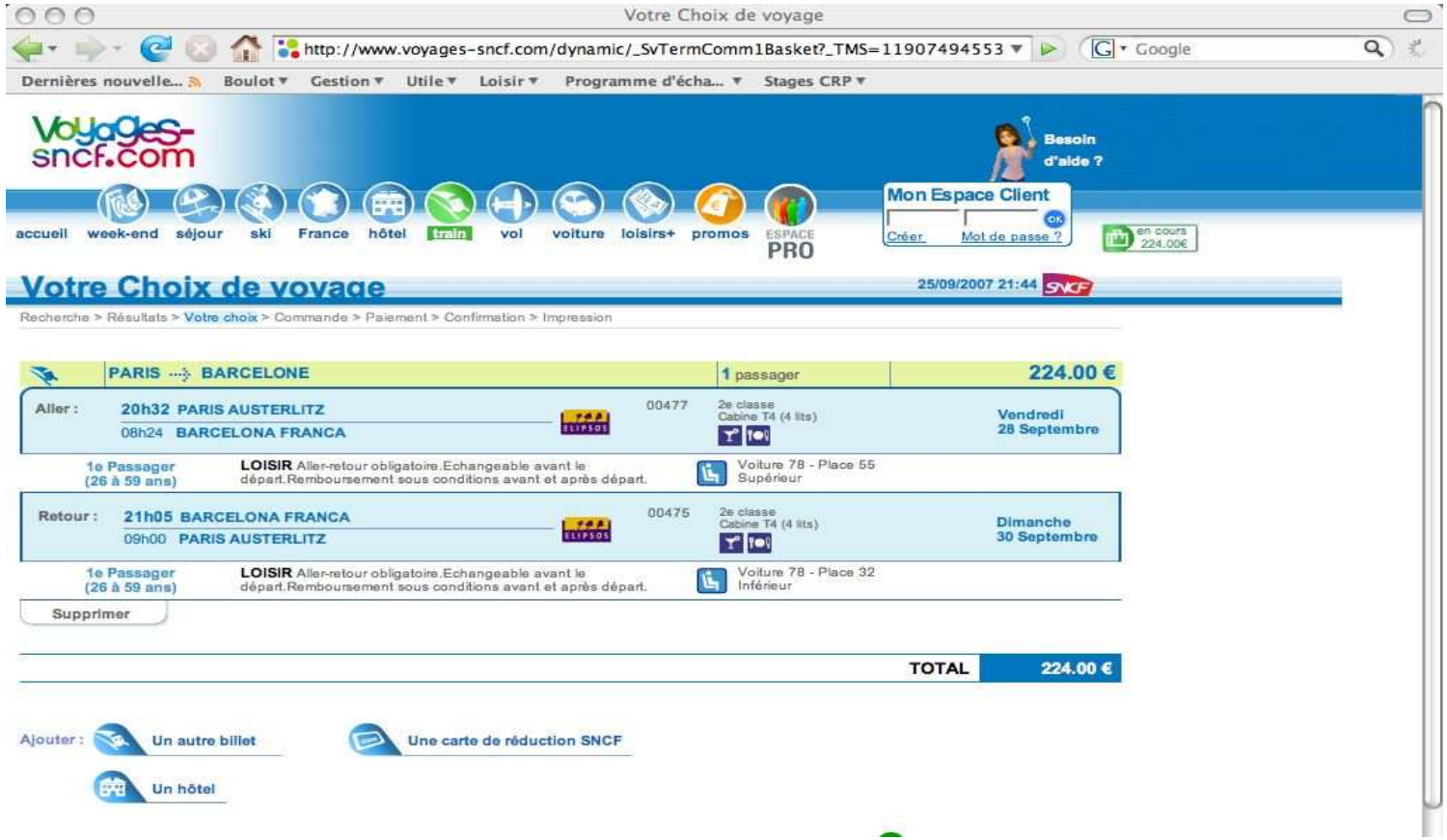
Mireille Fouquet

Université Paris Diderot

Journée de la fondation Sciences Mathématiques de Paris centre

28 septembre 2007

Achats sécurisés sur internet



Problème : La SNCF et moi ne partageons pas un même secret pour chiffrer et déchiffrer nos communications.

Motivations

Protocole de Diffie-Hellman : Soit G un groupe cyclique à n éléments de générateur g.

Mireille Fouquet	transmission en clair	Voyages-sncf.com
choisit $a \in [1, n[$		choisit $b \in [1, n[$
calcule $K_A = g^a$		calcule $K_B = g^b$
	$K_A \longrightarrow$	
	$\longleftarrow K_B$	
calcule $K_{AB} = {K_B}^a$		calcule $K_{AB} = {K_A}^b$

Secret commun : $K_{AB} = g^{ab}$

Problème du logarithme discret = calculer x en connaissant g et g^x.

Exemple : Dans $\mathbb{Z}/11\mathbb{Z}$, si on pose $g = 2$ et $x = 8$ alors $g^x = 3 \mod 11$.
Comment retrouver x à partir de 2 et de 3 ?

WANTED

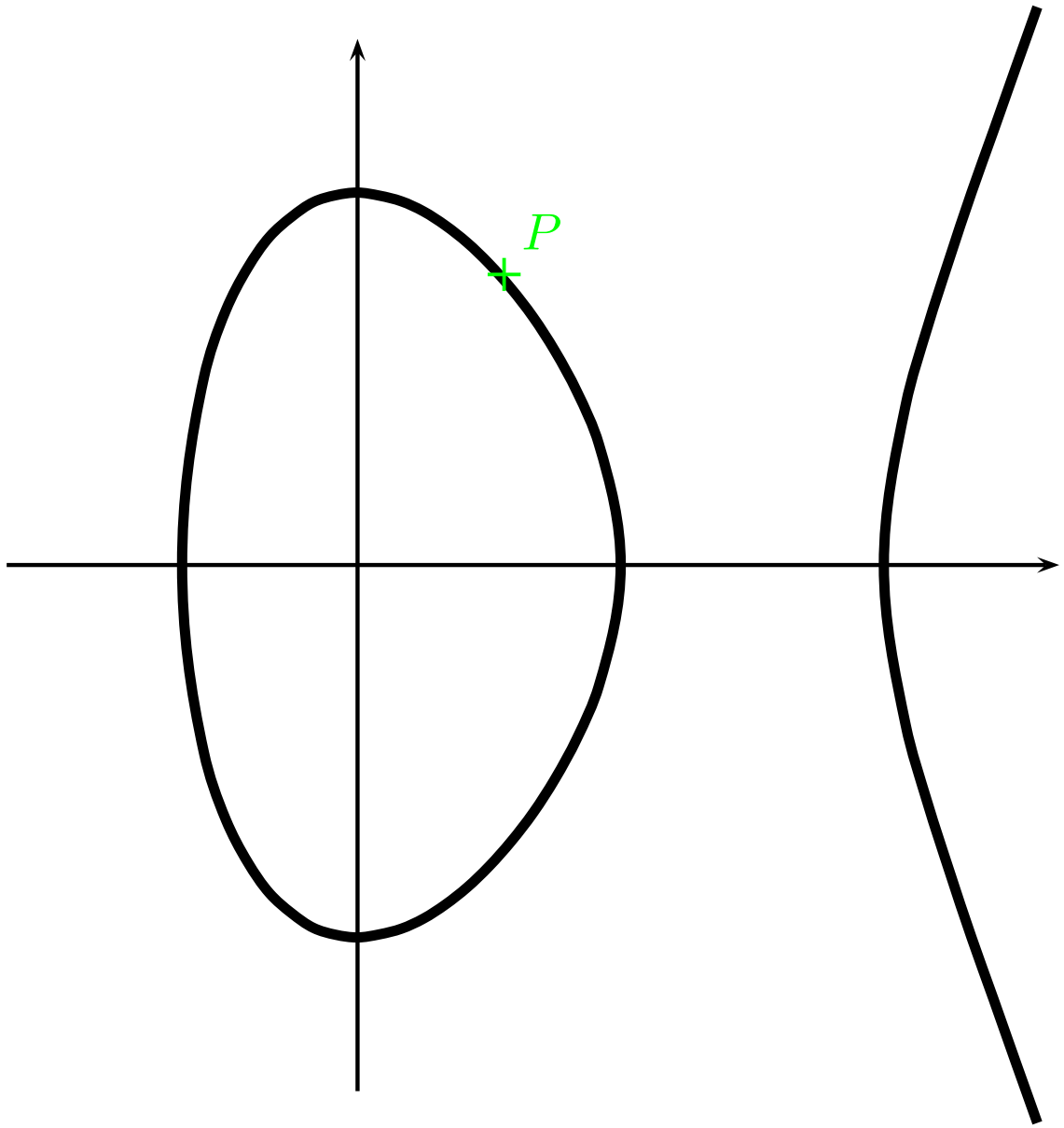
On cherche un groupe G tel que

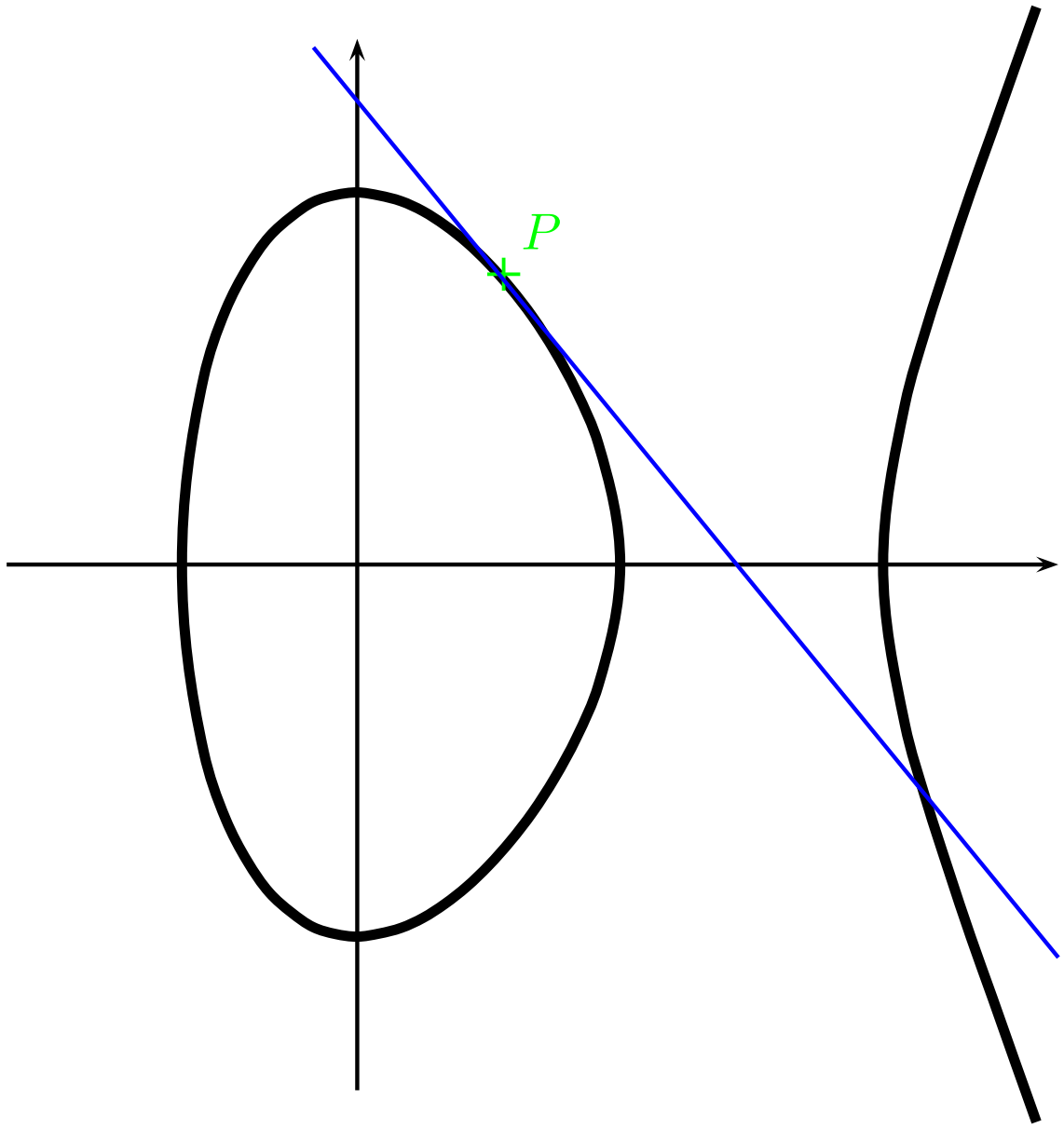
- calculer dans le groupe est simple ;
- résoudre le problème du logarithme discret est difficile dans le groupe.

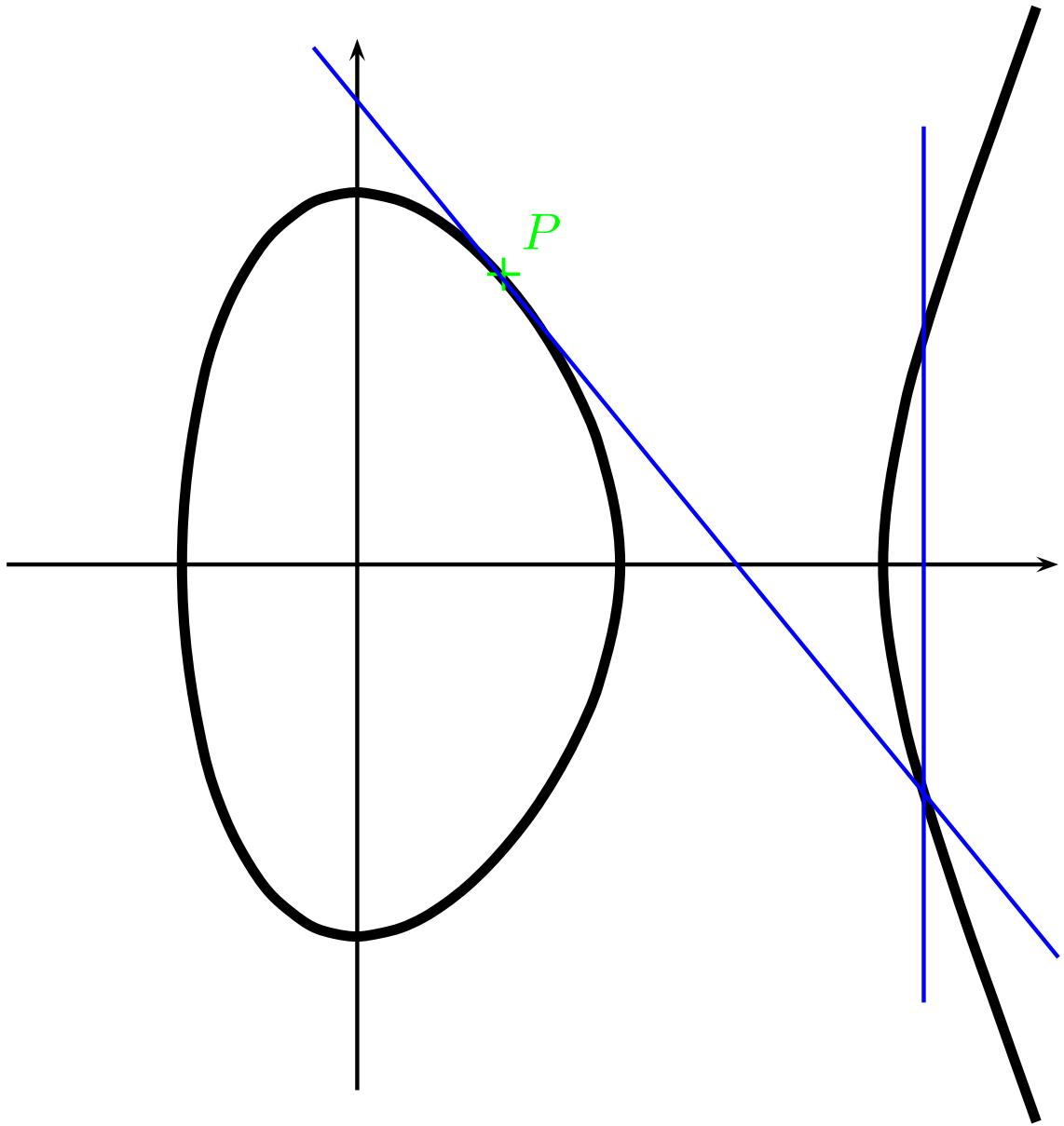
Candidat naturel : Groupe multiplicatif des corps finis (ex : $(\mathbb{Z}/11\mathbb{Z})^*$).

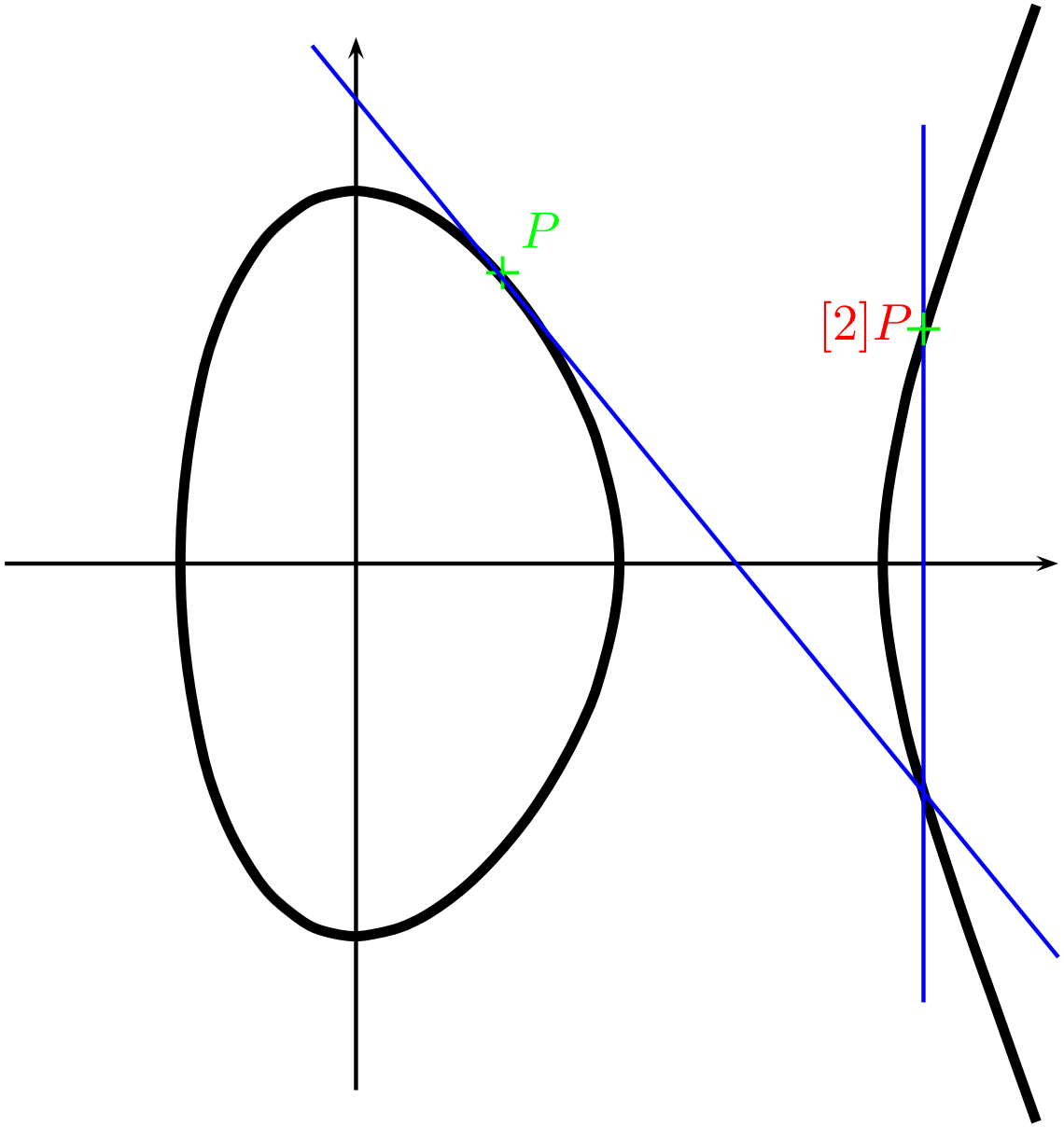
Utilisation en milieu contraint (carte à puce, organisateur électronique, téléphone portable, ...) : Nécessité d'un objet mathématique petit avec un même niveau de sécurité.

Bon candidat : Courbes elliptiques définies sur un corps fini.


P


P


P



Loi de groupe simple + pas d'attaque générale connue pour le log discret.

Axes de recherche

- Calculer le nombre de points d'une courbe elliptique sur un corps fini de manière efficace
- Vérifier l'invulnérabilité d'une courbe elliptique donnée aux attaques connues
- Étudier l'ensemble des invariants des courbes elliptiques afin de trouver de nouvelles attaques