Cryptographie et courbes elliptiques

Samuel Gallay

Rapport de stage de L3
sous la supervision de Vanessa Vitse

31 août 2022

Cryptographie symétrique et asymétrique

Cryptographie symétrique :

- Nécessite l'échange préalable d'une clef
- Est très rapide
- Résiste bien à l'ordinateur quantique

Cryptographie asymétrique :

- Ne nécessite pas d'échange préalable
- Est très lent
- Ne résiste pas à l'ordinateur quantique

Protocole de Diffie et Hellman

$$
\begin{tikzcd}
\textcolor{blue}{Alice} & \textcolor{red}{Bob} \\
a \arrow[d, blue] & b \arrow[d, red] \\
g^a \arrow[dr, blue] & g^b \arrow[dl, red] \\
g^b \arrow[d, blue] & g^a \arrow[d, red] \\
(g^b)^a \arrow[r, equal] & (g^a)^b
\end{tikzcd}
$$

Données publiques :

- G un groupe
- $n = \#G$
- g un générateur de G
- g^a et g^b après l'échange

Difficulté

Il faut que a soit difficile à trouver à partir de g^a.

Courbe elliptique

Caractéristique

K est un corps de caractéristique différente de 2 et de 3

$$E/K : y^2 = x^3 + ax + b \qquad a, b \in K$$

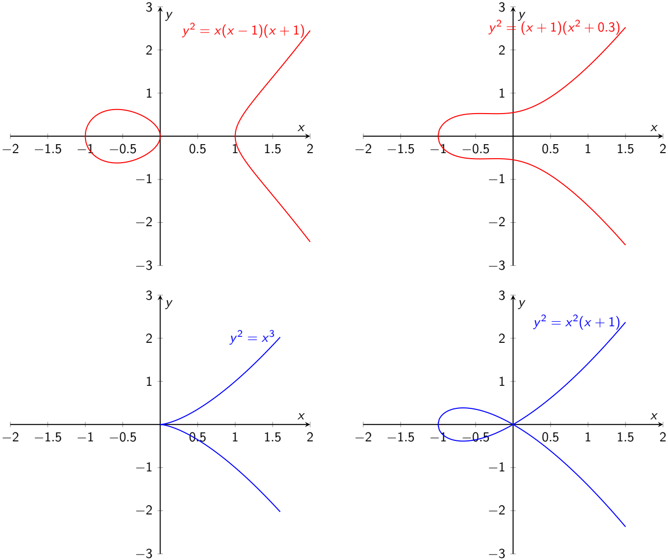
Solutions

On considère les solutions de l'équations dans $\overline{K}$, plus un point noté ∞

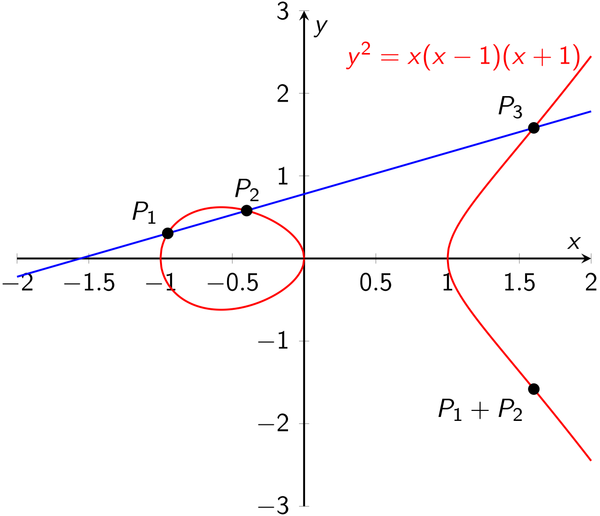
Discriminant

Le discriminant $\Delta = -16(4a^3 + 27b^2)$ doit être non nul

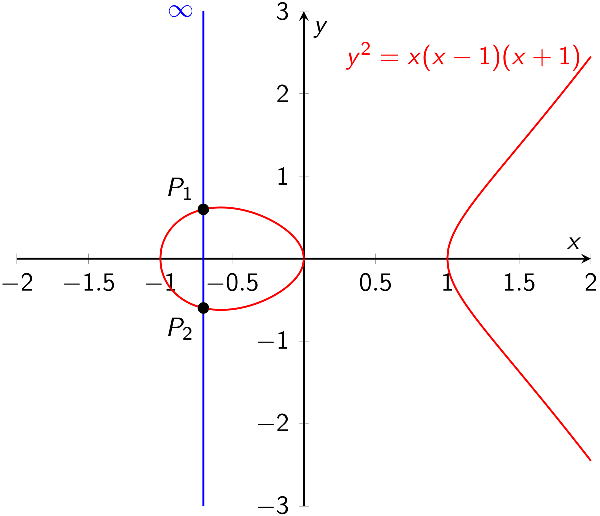
Exemple de courbes définies sur $\mathbb{R}$



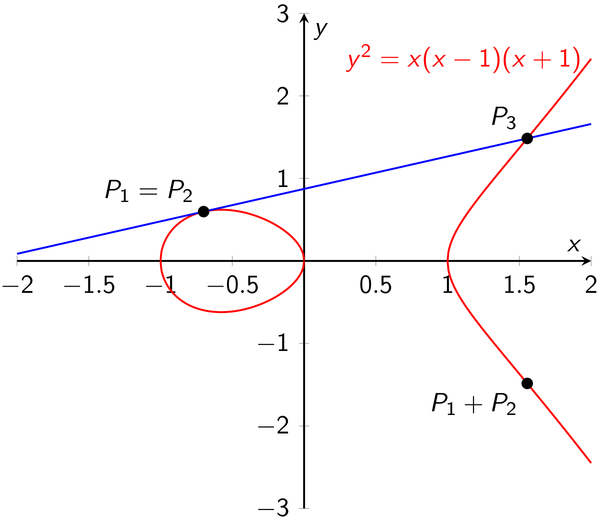
Addition de points I



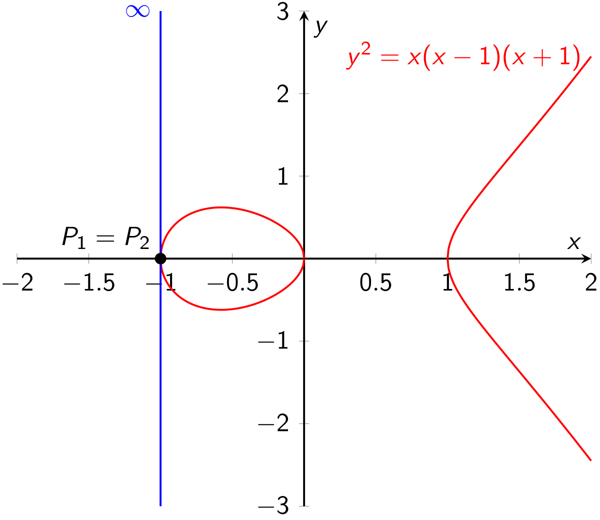
Addition de points II



Addition de points III



Addition de points IV



Loi de groupe et cryptographie

Groupe

$(E, \infty, +)$ est un groupe abélien

Cryptographie

On peut effectuer un Diffie-Hellman sur ce groupe !

Borne de Hasse

Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Alors $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.

Problème du logarithme discret

Définition

Étant donné un groupe G d'ordre n, un générateur g de ce groupe, et un élément h, trouver k tel que $h = g^k$.

Attaques standards

Les meilleures attaques

- Dans un groupe quelconque : algorithme ρ de Pollard en $O(\sqrt{n})$
- Dans $\mathbb{F}_q^\times$: calcul d'indice en $L_q(\frac{1}{2})$, Function Field Sieve en $L(\frac{1}{3})$
- Dans $E(\mathbb{F}_q)$: pas d'attaque meilleure que ρ de Pollard

$$L_n(\alpha, c) = e^{c(\log n)^\alpha (\log \log n)^{1-\alpha}}$$

Attaques quantiques

Dans un futur peut-être pas si lointain...

l'ordinateur quantique !

Danger : l'algorithme de Shor

Attaque sur les protocoles RSA, et Diffie-Hellman sur $\mathbb{F}_q^\times$ et $E(\mathbb{F}_q)$ en $O((\log n)^2(\log\log n)(\log\log\log n))$

Besoin de nouveaux algorithmes. . .

c'est la cryptographie post-quantique !

Les morphismes entre courbes elliptiques

Définition : Morphisme

$E_1 : y^2 = x^3 + a_1 x + b_1 \qquad E_2 : y^2 = x^3 + a_2 x + b_2 \qquad \psi : E_1 \to E_2$

$\psi(x,y) = (R_1(x,y), R_2(x,y)) \qquad \psi(\infty_{E_1}) = \infty_{E_2}$

R_1 et R_2 des fractions rationnelles

Premier théorème magique

Un morphisme de courbes elliptiques induit un morphisme de groupes entre E_1 et E_2.

Deuxième théorème magique

Un morphisme non constant est surjectif

Isogénies

Définition

Une isogénie est un morphisme non constant.

Multiplication

Pour $k \in Z$, si $k \neq 0$, l'application multiplication par k notée $[k] : E \to E$ est une isogénie.

Maintenant $K = \overline{\mathbb{F}}_p$.

Morphisme de Frobenius

L'application $\pi_q : E \to E^{(p)}$ définie par $\pi_p(x, y) = (x^p, y^p)$ est une isogénie.

Courbes supersingulières

Torsions

Soit $k \in \mathbb{Z}$. La k-torsion de E est le noyau de $[k]$ et est notée $E[k]$.

Courbes supersingulières

Une courbe $E/\overline{\mathbb{F}}_p$ est dite supersingulière si sa p-torision est triviale.

Théorème

Toute courbe supersingulière est $\overline{\mathbb{F}}_p$-isomorphe à une courbe définie sur $\mathbb{F}_{p^2}$.

L'article à étudier

Towards quantum-resistant cryptosystems
from supersingular elliptic curve isogenies

Luca de Feo, David Jao & Jérome Plût

On peut maintenant comprendre le titre de l'article !

Graphe des isogénies

Isogénie duale

Soit $\psi : E_1 \to E_2$ une isogénie. Il existe une unique isogénie $\widehat{\psi} : E_2 \to E_1$ telle que $\widehat{\psi} \circ \psi = [\deg \psi]$. C'est l'isogénie duale de ψ.

Relation d'équivalence

L'existence d'une isogénie entre deux courbes est une relation d'équivalence.

Construction du graphe d'isogénies

- Les noeuds sont les classes de $\overline{\mathbb{F}}_p$-isomorphismes des courbes elliptiques définies sur $\mathbb{F}_{p^2}$
- Deux classes sont reliées lorsqu'elles possèdent une isogénie entre elles

L'échange de clefs

$$
\begin{tikzcd}
 & E_A \arrow[dd, shift right, blue] \arrow[r, red, "\mathrm{Ker}(\phi'_B)=\langle m_B\phi_A(P_B)+n_B\phi_A(Q_B)\rangle", "\phi'_B"'] & E_{BA} \arrow[d, leftrightsquigarrow, "\wr"] \\
E_0 \arrow[ur, blue, "\mathrm{Ker}(\phi_A)=\langle m_A P_A+n_A Q_A\rangle", "{\phi_A,\ \phi_A(P_B),\ \phi_A(Q_B)}"'] \arrow[dr, red, "{\phi_B,\ \phi_B(P_A),\ \phi_B(Q_A)}", "\mathrm{Ker}(\phi_B)=\langle m_B P_B+n_B Q_B\rangle"'] & & E_{AB} \\
 & E_B \arrow[uu, shift right, red] \arrow[ur, blue, "\phi'_A", "\mathrm{Ker}(\phi'_A)=\langle m_A\phi_B(P_A)+n_A\phi_B(Q_A)\rangle"'] &
\end{tikzcd}
$$

Attaques récentes (août 2022)

Tout semblait en bonne forme avant début août. NIST Post-Quantum Cryptography (PQC) standardization process :

- 1st round (2017)—69 candidates
- 2nd round (2019)—26 surviving candidates
- 3rd round (2020)—7 finalists, 8 alternates
- 4th round (2022)—3 finalists and 1 alternate selected as standards. SIKE and three additional alternates advanced to a fourth round.

Quand tout à coup : *An efficient key recovery attack on SIDH*
Wouter Castryck et Thomas Decru

Conclusion

À retenir :

- Les courbes elliptiques sont un domaine de recherche riche et actif
- Elles sont bien adaptées à la cryptographie actuelle (et utilisées partout)
- Par contre la cryptographie post-quantique, comme SIDH, est difficile (et on y comprend pas grand-chose)
- Finalement les mathématiciens et cryptologues ne sont pas près d'être au chomage !

Bibliographie I

Wouter Castryck et Thomas Decru :
An efficient key recovery attack on sidh (preliminary version).
Cryptology ePrint Archive, Paper 2022/975, 2022.
URL https://eprint.iacr.org/2022/975.
https://eprint.iacr.org/2022/975.

Luca De Feo, David Jao et Jérôme Plût :
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.
J. Math. Cryptol., 8(3):209–247, 2014.
ISSN 1862-2976.
URL https://doi.org/10.1515/jmc-2012-0015.

Bibliographie II

Joseph H. Silverman :
The arithmetic of elliptic curves, volume 106 de *Graduate Texts in Mathematics*.
Springer-Verlag, New York, 1992.
ISBN 0-387-96203-4.
Corrected reprint of the 1986 original.

Lawrence C. Washington :
Elliptic curves.
Discrete Mathematics and its Applications. Chapman & Hall/CRC, second édition, 2008.
ISBN 978-1-4200-7146-7 ; 1-4200-7146-7.
URL https://doi.org/10.1201/9781420071474.
Number theory and cryptography.