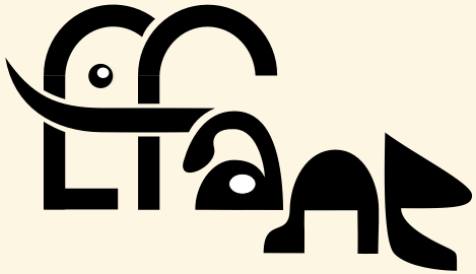
Elliptic Curves and Cryptography

2017/06 – **Mini-cours Agreg** – Lille

Damien Robert



Outline

1. Courbes elliptique
2. Fonctions sur les courbes
3. Algorithme de Miller
4. Couplages

Courbe plane lisse (k alg clos)

- Une courbe plane affine $C \subset \mathbb{A}_k^2 : f(x,y) = 0$ est lisse ssi en tout point $P = (x_P, y_P) \in C(k)$ on a

$$(\frac{\partial f}{\partial x}(x_P, y_P), \frac{\partial f}{\partial y}(x_P, y_P)) \neq (0,0).$$

- C admet alors une tangent en P d'équation

$$\frac{\partial f}{\partial x}(x_P, y_P)(x - x_P) + \frac{\partial f}{\partial y}(x_P, y_P)(y - y_P) = 0.$$

- Version projective : $C \subset \mathbb{P}_k^2 : F(X,Y,Z) = 0$ est lisse ssi en tout point $P = (X_P : Y_P, Z_P)$ de $C(k)$ on a

$$(\frac{\partial F}{\partial X}(X_P, Y_P, Z_P), \frac{\partial F}{\partial Y}(X_P, Y_P, Z_P), \frac{\partial F}{\partial Z}(X_P, Y_P, Z_P)) \neq (0,0,0).$$

- La tangente en P a pour équation

$$\frac{\partial F}{\partial X}(X_P, Y_P, Z_P)X + \frac{\partial F}{\partial Y}(X_P, Y_P, Z_P)Y + \frac{\partial F}{\partial Z}(X_P, Y_P, Z_P)Z = 0.$$

Courbes elliptiques ($\mathrm{char}\, k > 3$)

- Une courbe elliptique E/k est une courbe plane lisse d'équation affine

$$y^2 = f_E(x) = x^3 + ax + b.$$

- Il faut donc que f_E et f'_E n'aient pas de racines commune, ie $\mathrm{Disc} f_E = 4a^3 + 27b^2 \neq 0$.
- Équation projective : $Y^2Z = X^3 + AXZ^2 + bZ^3$;
- Point à l'infini : $0_E = (0:1:0)$, tangente en 0_E : $Z = 0$, le cercle à l'infini.

Cardinal de $E/\mathbb{F}_q$

- $E[\ell](\bar{k}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$;
- Sur $\mathbb{F}_q$, $E(\mathbb{F}_q) = \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ avec $a \mid b$;
- Polynôme caractéristique du Frobenius :

$$\chi_\pi(X) = (X-\pi)(X-\hat{\pi}) = X^2 - tX + q.$$

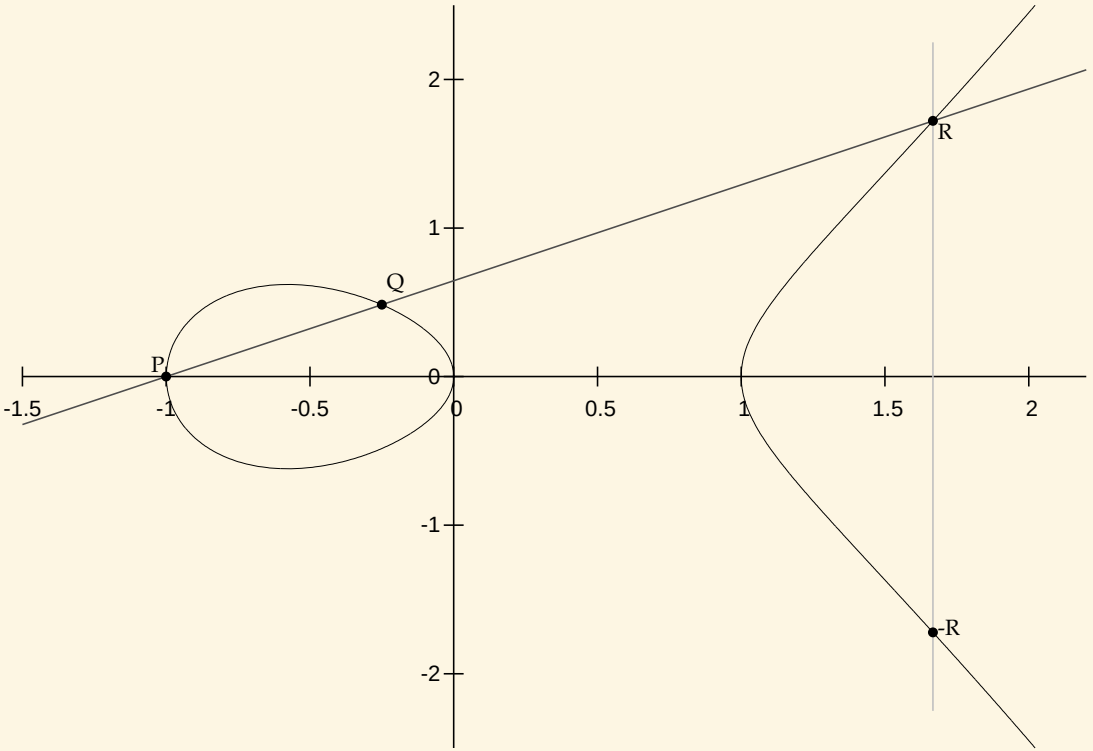
- Hasse : $|t| \leq 2\sqrt{q}$, donc $\Delta_\pi = t^2 - 4q \leq 0$.
- $\#E(\mathbb{F}_q) = \chi_\pi(1) = q + 1 - t$.

Logarithme discret

Définition ($\mathrm{char}\, k \neq 2, 3$)

Une courbe elliptique est une courbe plane d'équation :

$$y^2 = x^3 + ax + b \qquad 4a^3 + 27b^2 \neq 0.$$



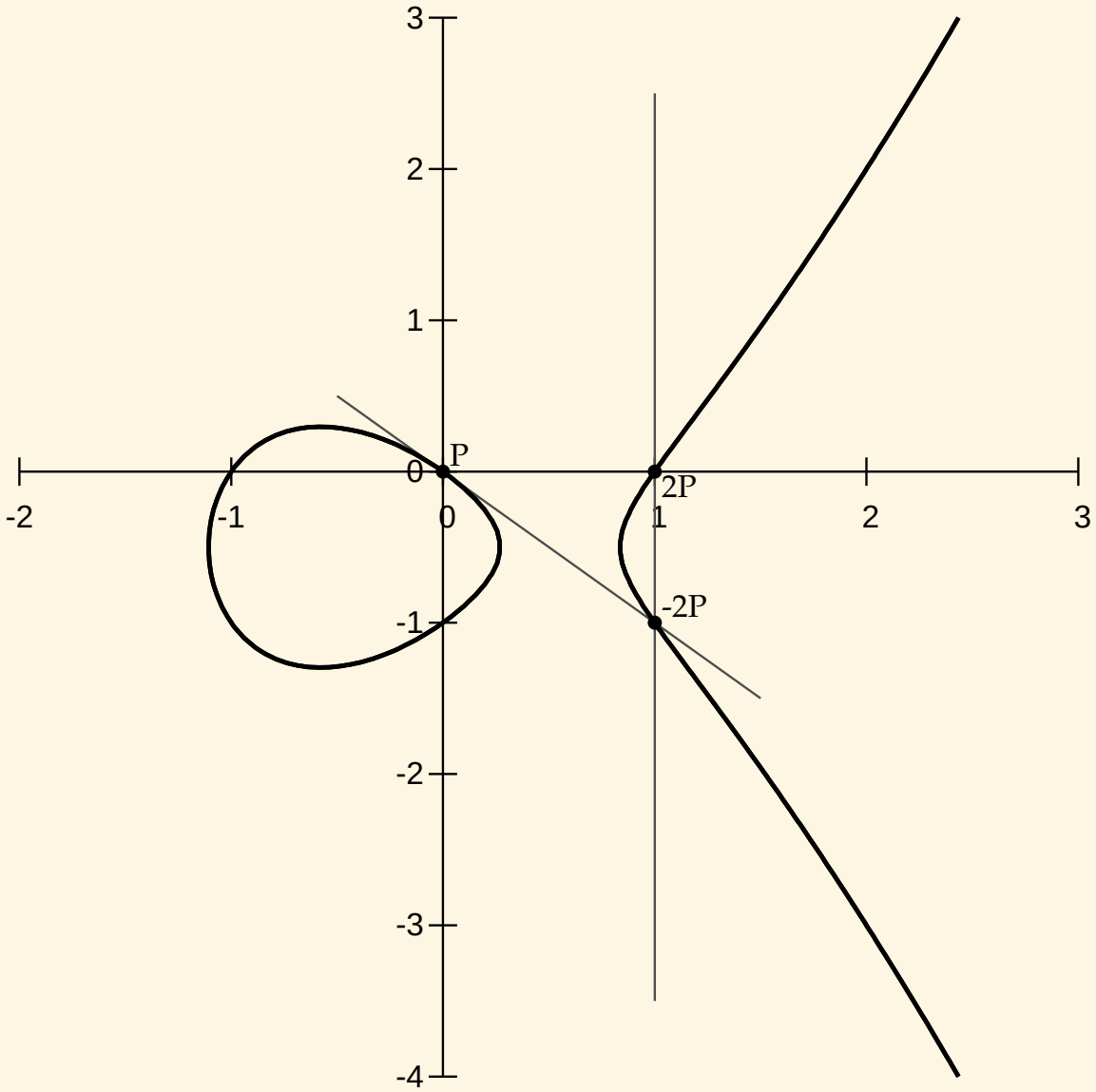
Exponentiation :

$$(\ell, P) \mapsto \ell P$$

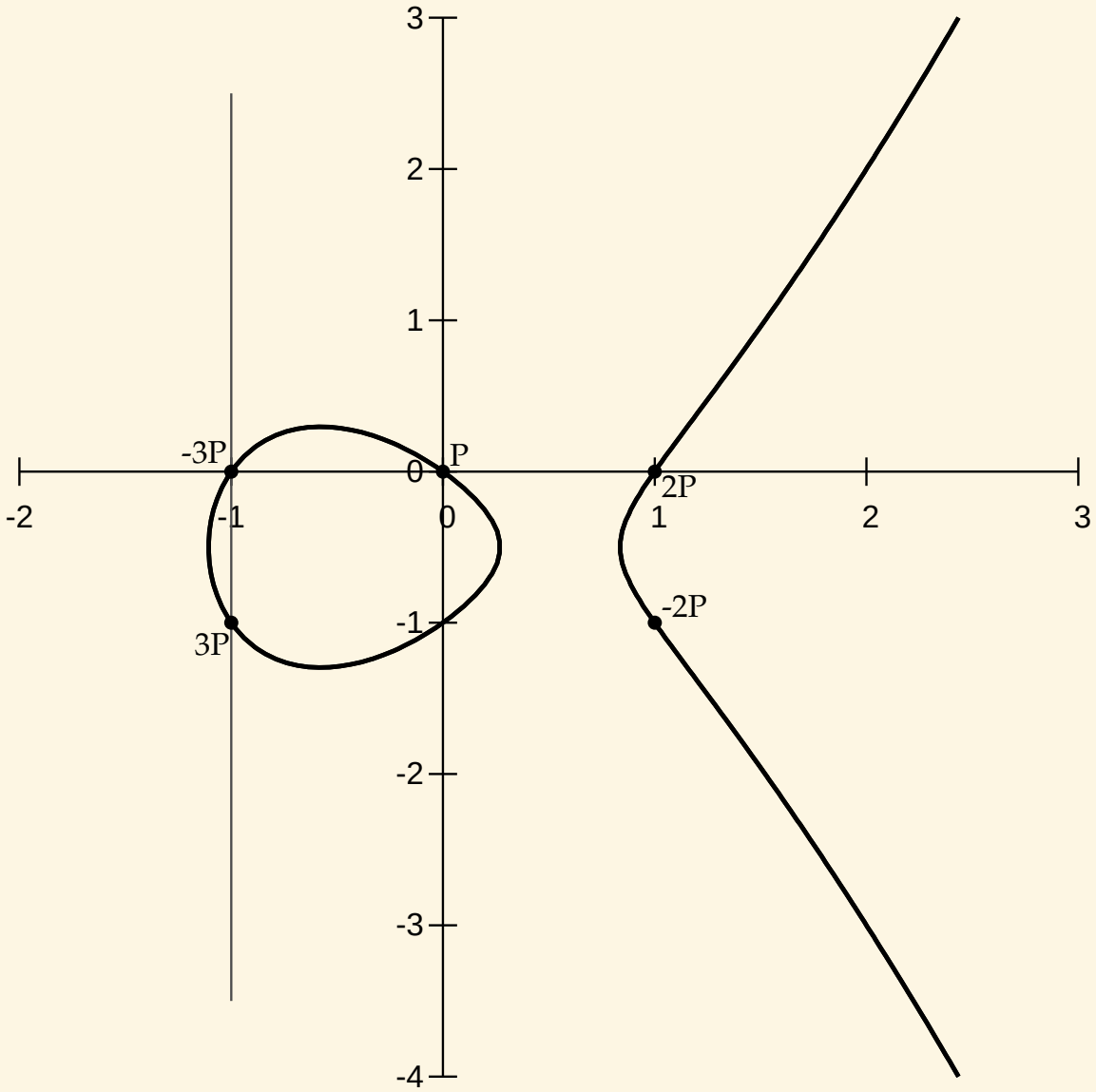
Logarithme discret :

$$(P, \ell P) \mapsto \ell$$

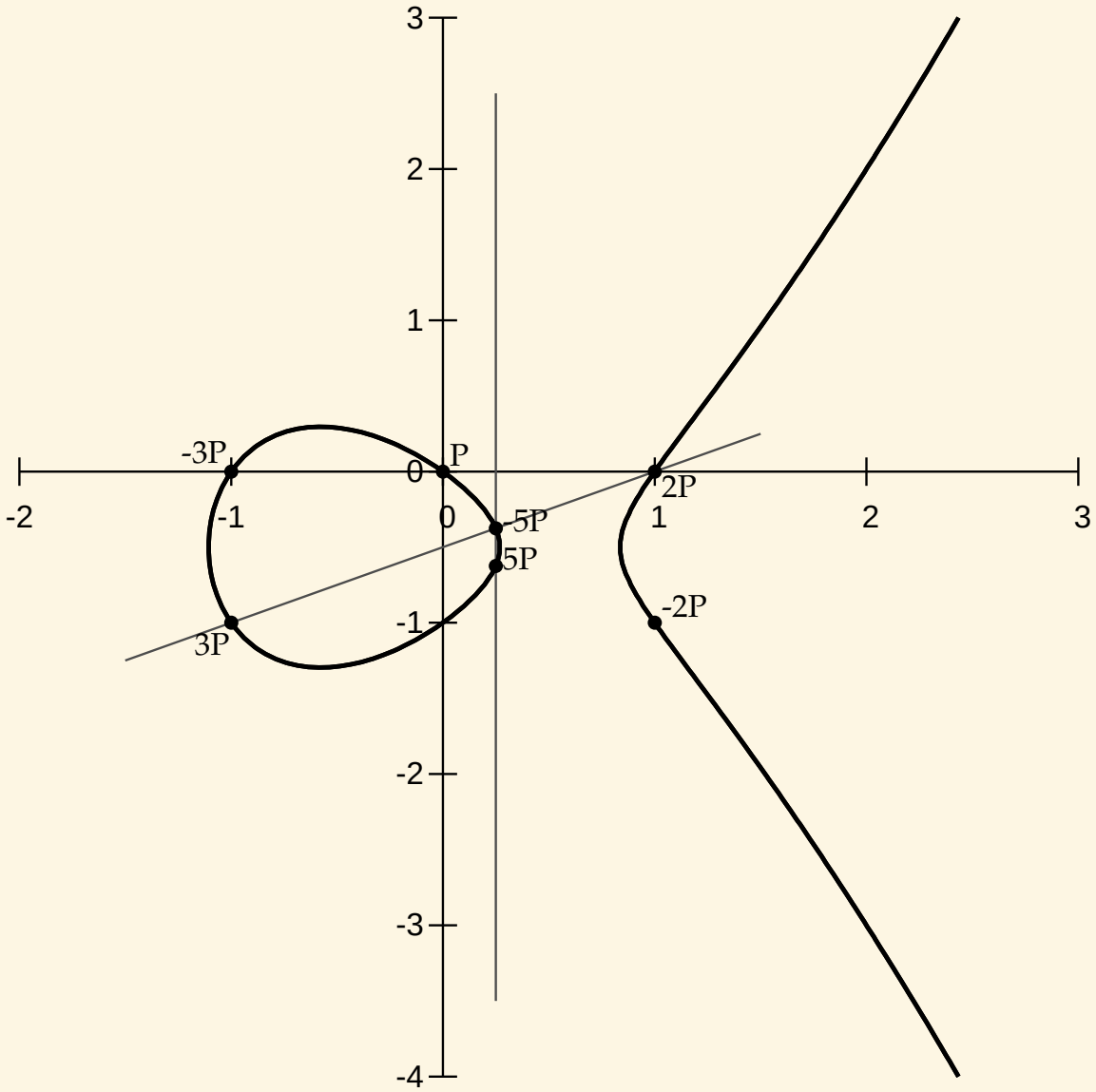
Multiplication scalaire sur une courbe elliptique



Multiplication scalaire sur une courbe elliptique



Multiplication scalaire sur une courbe elliptique



ECC (Elliptic curve cryptography)

Exemple (NIST-p-256)

- E courbe elliptique $y^2 =$
  $x^3 - 3x + 41058363725152142129326129780047268409114441015993725554835256314039467401291$
  sur $\mathbb{F}_{115792089210356248762697446949407573530086143415290314195533631308867097853951}$
- Clé publique :
  $P = (48439561293906451759052585252797914202762949526041747995844080717082404635286,$
  $36134250956749795798585127919587881956611106672985015071877198253568414405109),$
  $Q = (76028141830806192577282777898750452406210805147329580134802140726480409897389,$
  $85583728422624684878257214555223946135008937421540868848199576276874939903729)$
- Clé privée : ℓ tel que $Q = \ell P$.

ECC vs RSA pour 128 bits de sécurité

- ECC (Curve25519) 256 bits :

AAAAC3NzaC1lZDI1NTE5AAAAIMoNrNYhU7CY1Xs6v4Nm1V6oRHs/FEE8P+XaZ0PcxPzz

- RSA 3248 bits :

MIIHRgIBAAKCAZcAvlGW+b5L2tmqb5bUJMrfLHgr2jga/Q/8IJ5QJqeSsB7xLVT/
ODN3KNSPxyjaHmDNdDTwgsikZvPYeyZWWFLP0B0vgwDqQugUGHVfg4c73ZolqZk6
1nA45XZGHUPt98p4+ghPag5JyvAVsf1cF/VlttBHbu/noyIAC4F3tHP81nn+lOnB
eilEALbdmvGTTZ5jcRrt4IDT5a4IeI9yTe0aVdTsUJ6990hpKrVzyTOu1eoxp5eV
KQ7aIX6es9Xjnr8widZunM8rqhBW9EMmLqabnXZItPQoV3rUAnwKzDLV7E56viJk
S2xU5+95IctYu/RTTbf3wTxnkDOqxId0MONHyBJsukXgYKxVB1fWhBKZ4tWui1gw
UCIiKTqLml2zJhLn4WovaxrvvTx0082S0xncEfYDXYu4xbRnJn+ZsTTguqufwC1M
U4MYRdWy7uj+H1EmIGul69Fw9NkuCitWI9dFpcDtSP+/1eEN7wc2FlxhDIRwer0F
6I1P4StWn1uQyHzsTLVdcP+rqA1AsvbWBCKL4ravEO2CEQIDAQABAoIBllWt5YoJ
YZzk4RXbkSX/LvmWICfdmkjTKW6F1w+P4TnotCr0WPG0ObDoANJoUcnbSqNGMgCu
01SF8q9+UuDwZx4KBZm0j8IPOPzJ2nYcK5dYDhyMHzDq1LJ4zJfgPQGQ5WWq2BWm
2RHDhADdTth6YZArs/z9hAqtA9gqMPnMPcdQpIvlsHSOn06zBJD8sJQA+kOxG+Y2
GS8NakLcUVlDpNd/Q+QHkv4AW1ge2EF8QvmKtU/9rekOBqWNm2Tapd6RtAhZwPJX
UhD9yiesTF6rjZ1ZcMGXUaN5Rt0zD3D4zowRz2JLtCe4GkiJmtc3waN6hu1IaIqz
boI11evqnbatqnC4rCq8sf21yZqaLUIbwH4lW2G3K8xMJNh3iy8cgHTYneNYa+/d
7xyNWlMO9SKlHsyaPcWv98BdD+At0x/6R6YPYkeR+qXJ9ETGFKW4U6iNbBQXOMbh
kZb1Ry8vfMH8vsYIzh8Edg6aq00ScU57KiDS/Gc8KuqI6vmf2leCdCa487kVCgw6
cGXQ2bLZGYBiMZFfOOlpCQECgcwA5ZUh3/8yS0duNhsDz3sgC2u40HwHUbxuSOUa
a5t4CoUY9iuF7b7qhBEcvdLgIOiXA5xo+r4p0xgbLvDUTsRR1mrDM2+wRcjjwXcW
pFaMFRl2Rr72yLUC7N0WNcoUshrNL4X/1j8T4WLRcannpXcor+/kn1rwdLEbRCC+
zRTAdJlgMPt4kwJeHtE9Mzw2/O3GX3MeLvzvJklzvpCGw20N/2Yqjs++V5hXoHPs
21y6y6/FV097dvFctf7NahS04JsjubfnjOMx89AUNZsCgcwA1DfabCGJSCkmQ+mg
2q9lDPJz6r29wmBtYyT20oZ2kd4QBHrOp0t59yG4bvdRqcZG/Dr5LjuVDWMPyetV
dksK7hVYQz2B7Nzy7W3waPVrhA0N4fqbIFGxih5QiSFG7/oroZ8PdZDcfVRKroh1
/JJ7rIz/ZBQCLRS5t7/G2B0kBDOMMM+02wR60CTmxUhmgvsoDZWRp5KKha5PSvZa
WAu2CN3mXNK72RLF3RFUvuhNYnkOEj5Oau1RaGgpZoB0JTKYI9nffbe8up+DV8MC
gcwA18be28Ti5FXyg+/IGQ3EBHfucCTiTDQqA2Ew/8pTfK+z0kr9yYISsKXUuaSk
+skghkhPcrugW8LgabH4GT/zGu+lH4btyekSBxeCtFqTtpED1WJOWD2ozi7NXSjd
YrhF+VCcMCWA7ekOqSHjkmT4XMO/wPab4VFEKzgLnHzQlcZB3ke7/4/OHnDScIE7
vWVNeRCdYdRggT+wBX+Y6bxp142Smj8uyu1oDmpmR5ZUCnTdqT4O8K/RT0x4jCeC
CUhGv5rVillO7bS4CdkCgctXvnQwCzmwvVrV744TfTuhu8lTwHnqGWaA/LKU3wW9
T/x9ba1uHFXkaWvRba61LIcDGPsYM4hwTYokqYnfbC2rvOWOf6rtnXlP1An3y6lV
ovQfgDeNiFmIyvnviPPEm0JZA+QnburLYwOx4DgwYvyBnpal8WPo8c3L/J4hkwLm
Pc30DJ0xhUumLeyAnCyOcjygSfw8NenSVfzw+KIoDIeKaP0rWfJTUWDAAZ9yY6tD

Chiffrement El Gamal

- Clé publique : $(g, p = g^a)$, Clé privée : a ;
- Chiffrement $m \longmapsto (g^k, s = p^k . m)$ (k aléatoire) ;
- Déchiffrement $m = s/(g^k)^a$.
- Attention : Ne jamais réutiliser k.

Remarque (Diffie-Hellman)

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

Authentification sans divulgation de connaissances (Zero Knowledge)

- Alice publie $(g, p = g^a)$, son secret est a.
- Alice choisit un x aléatoire en envoie $q = g^x$;
- Soit Bob demande la valeur de $a + x$ et vérifie que $q \cdot p = g^{a+x}$.
- Sinon Bob demande la valeur de x et vérifie que $q = g^x$;

DSA (Signature)

- Clé publique : $(g, p = g^a)$, Clé privée : a ;
- $\Phi : G \to \mathbb{Z}/n\mathbb{Z}$;
- Signature : $m \mapsto (u = \Phi(g^k), v = (m + a\Phi(g^k))/k) \in (\mathbb{Z}/n\mathbb{Z})^2$;
- Vérification : $u = \Phi(g^{mv^{-1}} p^{uv^{-1}})$.

Loi d'addition sur le modèle de Weierstrass

$E : y^2 = x^3 + ax + b$ (forme Weierstrass courte).

- Quand $P \neq Q$:

$$P + Q = -R = (x_R, -y_R)$$

$$\alpha = \frac{y_Q - y_P}{x_Q - x_P}$$

$$x_R = \alpha^2 - x_P - x_Q \quad y_R = y_P + \alpha(x_R - x_P)$$

(Si $x_P = x_Q$ alors $P = -Q$ et $P + Q = 0_E$).

- Si $P = Q$, alors α est la pente de la tangente en P :

$$\alpha = \frac{3x_P^2 + b}{2y_P}$$

$$x_R = \alpha^2 - 2x_P \quad y_R = y_P + \alpha(x_R - x_P)$$

- Preuve : $l_{P,Q} : y - y_P = \alpha(x - x_P) + \beta$ équation de la droite entre P et Q (ou de la tangente à E en P quand $P = Q$). De plus x_R, x_P, x_Q sont les trois racines $x^3 + ax + b - (\alpha x + \beta)^2$ donc $x_P + x_Q + x_R = \alpha^2$.

$\Rightarrow$ Travailler en coordonnées projective $(X : Y : Z)$ évite de calculer les divisions :

$$E : Y^2 Z = X^3 + aXZ^2 + bZ^3.$$

Multiplication scalaire

- $P \longmapsto n.P$ par l'algorithme « double and add » ;
- Exemple : $22 = 2^4 + 2^2 + 2 = (2(1+2(2)))$. $22.P = \overline{10110}.P$: Double, Double+Add, Double+Add, Double $\Rightarrow P$, $2P$, $5P$, $11P$, $22P$;
- En moyenne $\log n$ doublement et $1/2 \log n$ additions ;
- Améliorations : windowing. $\overline{10110}.P$: Double+Double+Add P, Double+Double+Add $2P \Rightarrow 5P$, $22P$;
- Fenêtre de taille $k \Rightarrow$ table de taille 2^k, $\log n$ doublements et $1/k(1-1/2^k)\log n$ additions ;
- Sliding window : Double, Double, Double, Add $3P$, Double $\Rightarrow P$, $2P$, $4P$, $8P$, $11P$, $22P$;
- Fenêtre de taille $k \Rightarrow$ table de taille 2^{k-1}, $\log n$ doublements et $1/(k+1)\log n$ additions ;
- NAF (non adjacent form), $n = \sum b_i 2^i$ où $b_i \in \{-1, 0, 1\}$. On a toujours une représentation sans deux $1, -1$ consécutifs $\Rightarrow \log n$ doublement et $1/3 \log n$ additions/soustractions.
- $22 = 32 - 8 - 2 = \overline{10\text{-}10\text{-}10}$. $22.P$: Double, Double+Subtract, Double, Double+Subtract, Double $\Rightarrow P$, $2P$, $3P$, $6P$, $11P$, $22P$.

Multiplications scalaires

- Multiples scalaires $(P,Q) \longmapsto n.P + m.Q$ par doublement et addition de P, Q ou $P+Q$ suivant les bits de n et m ;
- En moyenne $\log N$ doublement et $3/4 \log N$ additions où $N = \max(n,m)$;
- GLV : s'il existe un endomorphisme α (calculable facilement) tel que $\alpha(P) = u.P$ where $u \approx \sqrt{n}$, alors on peut remplacer le calcul de $n.P$ par un calcul $n_1 P + n_2 \alpha(P)$;
- On s'attend à ce que n_1 et n_2 soit de taille la motiée de celle de $n \Rightarrow$ de $\log n$ doublement et $1/2 \log n$ additions à $1/2 \log n$ doublement et $3/8 \log n$ additions.

Fonctions rationnelles sur la droite projective

- Soit C la droite projective $\mathbb{P}^1_k$ sur k (k alg. clos), $K = k(C) = k(X)$ son corps des fonctions ;
- Si $P = (a:1) \in C(k)$ et $f \in k(C)$, on définit $v_P(f) = n$ ssi $f = (X-a)^n f_0$ où P n'est pas un pôle ni un zéro de P ;
- $v_P : k(C) \to \mathbb{Z}$ est une valuation discrète

$$v_P(fg) = v_P(f) + v_P(g)$$
$$v_P(f+g) \geq \min(v_P(f), v_P(g))$$
$$v_P(f+g) = \min(v_P(f), v_P(g) \text{ si } v_P(f) \neq v_P(g).$$

  $v_P(X-a) = 1$ donc $X-a$ est une uniformisante en P.
- Si $v_P(f) = 0$, P n'est pas un pôle ou zéro de f ;
- Si $v_P(f) = n > 0$, P est un zéro d'ordre (ou de multiplicité) n de f ;
- Si $v_P(f) = n < 0$, P est un pôle d'ordre (ou de multiplicité) n de f.

Remarque

$f \in k(X)$ a un développement en série de Laurent

$$f = \sum_{i \geq v_a(f)} c_i (X-a)^i$$

.

Point à l'infini

- Si $\infty = (1:0)$ est le point à l'infini, on définit $v_\infty(f(X)) = v_0(f(1/X))$;
- Si $f(X) = f_1(X)/f_2(X)$, $v_\infty(f) = \deg f_2 - \deg f_1 = -\deg f$;

- Les valuations discrètes (non triviales) sur $k(C) = k(X)$ sont en bijection avec les points $C(k) = \mathbb{P}^1_k(k)$;

- Remarque : si $k = \mathbb{R}$, la valuation correspondant à l'uniformisante X^2+1 correspond au point schématique $\mathrm{Spec}\,\mathbb{R}[X]/(X^2+1)$ ou encore à l'orbite Galoisienne $\{i,-i\}$ dans $\mathbb{P}^1_{\mathbb{R}}(\mathbb{C})$.

Diviseurs

- Si $f \in k(C)$, on définit la somme formelle

$$\mathrm{div}(f) = \sum_{P \in C(k)} v_P(f)(P);$$

- Un diviseur est une somme formelle à support fini $D = \sum_{P \in C(k)} n_P(P)$;
- Si $D = \sum_{P \in C(k)} n_P(P)$ est un diviseur, son degré est $\deg(D) = \sum_{P \in C(k)} n_P$;
- $\mathrm{div}(f)$ est un diviseur de degré 0 ;
- Exemple : $f = c\frac{\prod (X-a_i)^{n_i}}{\prod (X-b_i)^{m_i}}$ a pour diviseur $\sum n_i(a_i) - \sum m_i(b_i) - \deg f(\infty)$;
- Réciproquement si $D = \sum n_i(a_i) + m(\infty)$ est un diviseur de degré 0, $f = \prod (X-a_i)^{n_i}$, $\mathrm{div} f = D$.

Proposition

$\mathrm{div}(f) = \mathrm{div}(g)$ *ssi* $f = cg$ *où* $c \in k$.

Courbes

- $C \longmapsto k(C)$ donne une équivalence de catégorie entre les courbes (intègres) + les morphismes dominants et la catégorie opposée des corps K de degré de transcendance 1 sur k (et de type fini sur k) ;
- Si K est un corps de degré de transcendance 1 sur k, K correspond à une classe d'équivalence birationnelle d'une courbe C. Il existe un unique représentant projectif lisse $\widetilde{C}$ de cette classe (que l'on peut obtenir par résolution des singularités en faisant des blowups sur C) ;
- On suppose dorénavant que C est une courbe intègre lisse.

Exemple ($\mathrm{char}\, k > 3$)

Si $E : ZY^2 = X^3 + aXZ^2 + bZ^3$ est une courbe elliptique, c'est une courbe projective lisse intègre représentant le corps $k(E) = k(x)[y]/(y^2 - x^3 - ax - b)$.

Valuations

Théorème

Si C est une courbe intègre lisse projective sur k (alg. clos), il y a bijection entre les points $C(k)$ et les valuations discrètes (non triviales) sur $k(C)$.

Démonstration.

Dans un sens : si $P \in C(k)$, on peut définir O_P l'anneau local donné par les fonctions de $C(k)$ définies en P, m_P son idéal maximal donné par les fonctions s'annulant en P.
Comme C est lisse, $\dim_k m_P/m_P^2 = 1$, donc (O_P, m_P) est un anneau de valuation discrète. □

- On a donc $m_P = (t_P)$ où t_P est une uniformisante en P.
- Si $f \in k(C)$ on peut écrire $f = t_P^{v_P(f)} f_0$ avec $f_0(P) \notin \{0, \infty\}$, autrement dit $f_0 \in O_P^*$.

Interprétation géométrique

- Soit $C : f(x,y) = 0$ une courbe plane affine intègre lisse.
- Soit $g \in k[C] = k[x,y]/f(x,y)$, restriction d'une fonction $\tilde{g} \in k[x,y] = k(\mathbb{A}^2_k)$.
- Soit $P \in C$, et notons $m_P \subset k[C]$ l'idéal d'annulation en P dans $k[C]$ et $\tilde{m}_P \subset k[x,y]$ le même idéal dans $k[x,y]$.

$$\tilde{g}(x,y) = \tilde{g}(P) + \frac{\partial \tilde{g}}{\partial x}(x_P,y_P)(x-x_P) + \frac{\partial \tilde{g}}{\partial y}(x_P,y_P)(y-y_P) \mod \tilde{m}_P^2.$$

- Or $v_P(g) \geq 2$ ssi $g \in m_P^2$ ssi $\tilde{g} \in \tilde{m}_P^2 + (f)$ ssi C est tangente à la courbe associée à $\tilde{g}$ dans $\mathbb{A}^2_k$.

Complétion

Remarque (complétion)

Pour tout $P \in C(k)$, on a $k(C) \subset k((t_P))$ où t_P est une uniformisante en P :

$$f = \sum_{i=v_P(f)}^{\infty} a_i t_P^i.$$

On a $a_{v_P(f))} = (f t_P^{-v_P(f)})(P)$.

Exemple (Modèles de courbes elliptiques.)

- Soit C l'intersection des deux quadriques

$$u^2 + kw^2 = 1, v^2 - 4w^2 = 1.$$

- C a un point rationnel donc est une courbe elliptique.
- $x = \frac{1-u}{k-kw}$ et $y = wk^2/2$ donnent les coordonnées de Weierstrass.
- Le développement en série de Laurent permet de calculer l'équation de Weierstrass.

Diviseurs

- Si $f \in k(C)$, $\mathrm{div}(f) = \sum_{P \in C(k)} v_P(f)(P)$ est un diviseur de degré 0 ;
- $\mathrm{div}(f) = \mathrm{div}(g)$ ssi $f = cg$ où $c \in k$.
- Attention : si D est un diviseur de degré 0, D ne provient pas forcément d'une fonction f.
- Si $D = \mathrm{div}(f)$ on dit que D est un diviseur principal ;
- D est linéairement équivalent à D' ssi $D = D' + \mathrm{div}(f)$;
- D est linéairement équivalent à 0 ssi D est principal ;
- $\mathrm{Pic}(C) = \mathrm{Div}^0(C)/\mathrm{Princ}(C)$.

Évaluer une fonction en un diviseur

- Si $D = \sum n_P(P)$ est un diviseur et $f \in k(C)$ de support disjoint de D,

$$f(D) = \prod f(P)^{n_P}.$$

- On peut étendre l'évaluation $f(D)$ à tout D en posant $f(P) = a_{v_P(f)}$, le premier terme de la série de Laurent de f en t_P (dépend des uniformisantes choisies).

Théorème (Réciprocité de Weil)

$$f(\operatorname{div} g) = (-1)^{\sum_P v_P(f) v_P(g)} g(\operatorname{div} f)$$

Exemple

Si $C = \mathbb{P}^1_k$, $f, g \in k[X]$,
$f(\operatorname{div} g) = \operatorname{Res}(f,g) = (-1)^{\deg f \deg g}(g,f) = (-1)^{\deg f \deg g} g(\operatorname{div} f)$.

Fonctions sur les courbes elliptiques

- Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique (affine), $k(E)/k(x)$ est une extension Galoisienne de degré 2.
- On note σ l'involution Galoisienne et $N(f) = f \cdot \sigma(f) \in k(x)$ la norme de f ;
- Si $f(x,y) \in k(E) = k(x)[y]/(y^2 - x^3 - ax - b)$, on peut écrire $f = f_1(x) + y f_2(x)$ avec $f_1(x), f_2(x) \in k(x)$.

- Soit $\pi : E \to \mathbb{P}^1, (x,y) \mapsto x$ le revêtement Galoisien associé à $k(E)/k(x)$.
- Si $f \in k(x)$, $\operatorname{div} f = \sum n_i x_i$, $\pi^* \operatorname{div} f = \operatorname{div} \pi^* f = \operatorname{div} f \circ \pi = \sum n_i \pi^*(x_i)$.
- Si $f \in k(E), \operatorname{div} f = \sum n_P P$, $\pi_* \operatorname{div} f = \sum n_P \pi(P) = \operatorname{div} N(f)$.

- Si $P = (x_P, y_P) \in E(k)$ avec $y_P \neq 0$, une uniformisante est $t_P = (x - x_P)$;
- Si $P = (x_P, 0) \in E(k)$ est un point de Weierstrass, une uniformisante est $t_P = y$;
- Si $P = 0_E$, une uniformisante est $t_P = x/y$.

Remarque

$v_P(f) = v_{-P}(\sigma(f))$.

Calcul pratique de valuations

- Si P n'est pas un point de Weierstrass, et $f = f_1(x) + y f_2(x) \in k(E)$ vérifie $f(P) = f(-P) = 0$, alors $f_1(x_P) = f_2(x_P) = 0$, donc on a $f(x,y) = (x - x_P) f_0(x,y)$;
- Si $f \in k(E)$ elle s'écrit donc $f(x,y) = (x - x_P)^n f_0(x,y)$ avec soit $f_0(P) \neq 0$, soit $f_0(-P) \neq 0$, ie $\sigma(f_0)(P) \neq 0$. Dans le premier cas $v_P(f) = n$, et dans le second $f(x,y) = (x - x_P)^n \frac{N(f_0)}{\sigma(f_0)}(x,y)$ donc $P(f) = n + v_{x_P}(N(f_0))$.
- Si P est un point de Weierstrass, E a pour équation $y^2 = (x - x_P)(x - x_Q)(x - x_R)$. En particulier

$$x - x_P = \frac{y^2}{(x - x_Q)(x - x_R)},$$

  donc $v_P(x - x_P) = 2$.
- Si $f = f_1(x) + y f_2(x)$ alors $v_P(f_1)$ est pair et $v_P(y f_2)$ est impair donc $v_P(f)$ est le minimum des deux. On a $f = y^{v_P(f)} f_0$ avec $f_0(P) \notin \{0, \infty\}$, donc $v_P(f) = v_{x - x_P} N(f)$.
- $v_{0_E}(f) = -\deg(f)$ où $\deg(x) = 2$ et $\deg(y) = 3$.
- Ainsi $\operatorname{div}(x - x_P) = (P) + (-P) - 2(0_E)$.

$\mathrm{Pic}(E) \simeq E$

Théorème

- $D = \sum_{P \in E(k)} n_P(P)$ *est principal ssi*

$$\sum n_P P = 0_E \in E(k).$$

- *Si* $D = \sum_{P \in E(k)} n_P(P)$ *est de degré* 0, *alors* D *est linéairement équivalent à* $(\sum n_P(P)) - (0_E)$;

Remarque

Si D est principal, f une fonction représentant D : $D = \mathrm{div} f$. On peut normaliser f en demandant que $(f t_{0_E}^{-v_P(f)})(0_E) = 1$. On note f_D la fonction normalisée correspondante.

- Question : Étant donné un diviseur principal $D = \sum n_P(P)$, comment calculer f_D et évaluer rapidement $f_D(Q)$?
- Sur $\mathbb{P}^1_k$, $D = \sum n_i(a_i)$, $f_D(x) = \prod (x - a_i)^{n_i}$ s'évalue en temps (quasi) linéaire en la taille de D.

Exemple : $D = (P) + (Q) - (P+Q) - (0_E)$

- $D = (P) + (Q) - (P+Q) - (0_E)$ est principal, on note $\mu_{P,Q}$ la fonction normalisée associée.
- Soit $l_{P,Q}$ la droite passant par P et Q. On a $\operatorname{div} l_{P,Q} = (P) + (Q) + (-P-Q) - 3(0_E)$.
- Soit v_P la droite verticale passant par P, on a $\operatorname{div} v_P = (P) + (-P) - 2(0_E)$.
- Si $Q \neq -P$,

$$\mu_{P,Q} = \frac{l_{P,Q}}{v_{P+Q}} = \frac{y - \alpha(x - x_P) - y_P}{x + (x_P + x_Q) - \alpha^2}$$

où $\alpha = \frac{y_P - y_Q}{x_P - x_Q}$ est la pente de $l_{P,Q}$ ($\alpha = \frac{f'_E(x_P)}{2y_P}$ si $P = Q$ est la pente de la tangente en P).

- $\mu_{P,-P} = (x - x_P)$;

Cas général

- Si $D = (P) + (Q) + (R) + \cdots + m(0_E)$, on a $D - \mathrm{div}(\mu_{P,Q}) = (P+Q) + (R) + \cdots + (m+1)(0_E)$;
- Par itérations successive, on se ramène à un diviseur de la forme $(R) - (0_E)$.
- Si $R = 0_E$, D est principal. Sinon, D n'est pas principal, car si f avait pour diviseur $(R) - (0_E)$, on aurait $k(E) = k(f)$, donc E serait de genre 0, mais une courbe elliptique est de genre 1.
- Si $D = n_P(P) + n_Q(Q) + \cdots + m(0_E)$, on peut avoir beaucoup d'itérations successives.
- Si $P \in E(k)$, $D = \lambda(P) - (\lambda P) - (\lambda - 1)(0_E)$ est un diviseur principal, on note $f_{\lambda,P}$ la fonction associée. Comment évaluer la fonction $f_{\lambda,P}$ en un point Q rapidement ?
- Cas particulier : si $P \in E[\ell](k)$ est un point de ℓ-torsion (ℓ grand), comment évaluer la fonction $f_{\ell,P}$ de diviseur $\ell(P) - \ell(0_E)$ en un point Q rapidement ?

Cas général

- Si $D = (P) + (Q) + (R) + \cdots + m(0_E)$, on a $D - \mathrm{div}(\mu_{P,Q}) = (P+Q) + (R) + \cdots + (m+1)(0_E)$;
- Par itérations successive, on se ramène à un diviseur de la forme $(R) - (0_E)$.
- Si $R = 0_E$, D est principal. Sinon, D n'est pas principal, car si f avait pour diviseur $(R) - (0_E)$, on aurait $k(E) = k(f)$, donc E serait de genre 0, mais une courbe elliptique est de genre 1.
- Si $D = n_P(P) + n_Q(Q) + \cdots + m(0_E)$, on peut avoir beaucoup d'itérations successives.
- Si $P \in E(k)$, $D = \lambda(P) - (\lambda P) - (\lambda - 1)(0_E)$ est un diviseur principal, on note $f_{\lambda,P}$ la fonction associée. Comment évaluer la fonction $f_{\lambda,P}$ en un point Q rapidement ?
- Cas particulier : si $P \in E[\ell](k)$ est un point de ℓ-torsion (ℓ grand), comment évaluer la fonction $f_{\ell,P}$ de diviseur $\ell(P) - \ell(0_E)$ en un point Q rapidement ?

Algorithme de Miller

- $f_{\lambda+\nu,P} = f_{\lambda,P} f_{\nu,P} \mu_{\lambda P,\nu P}$
- En effet le diviseur du quotient est

$$(\lambda+\mu)P - ((\lambda+\mu)P) - \lambda(P) + (\lambda P) - \lambda(Q) + (\lambda Q) - (\lambda P) - (\lambda Q) + ((\lambda+\mu)P) + (0_E) \simeq 0.$$

- On en déduit un algorithme de « double and add » pour calculer $f_{\lambda,P}$. Initialisation : $f_{1,P} = 1$.

Algorithme

Input: $r \in \mathbb{N}$, $l = [\log r]$, $P = (x_P, y_P) \in E(k), Q = (x_Q, y_Q) \in E(k)$.

Output: $f_{r,P}(Q)$.

1. Compute the binary decomposition : $r := \sum_{i=0}^{l} b_i 2^i$. Let $T = P, f = 1$.
2. For i in $[l-1\,..0]$ compute
   1. $f = f^2 \mu_{T,T}(Q)$;
   2. $T = 2T$;
   3. If $b_i = 1$, then compute
      1. $f = f \mu_{T,P}(Q)$;
      2. $T = T + P$.

Return f.

Cryptographie à base de couplages

Définition

Un couplage est une application bilinéaire non dégénérée $e : G_1 \times G_1 \longrightarrow G_2$ entre des groupes abéliens finis.

Exemple

- Si le couplage e est facile à calculer, la difficulté du DLP dans G_1 se ramène à la difficulté du DLP dans G_2.

$\Rightarrow$ Attaque MOV sur les courbes elliptiques supersingulières : passage du DLP sur $E(\mathbb{F}_p)$ au DLP dans $(\mathbb{F}_p^2)^*$.

- One way tripartite Diffie–Hellman [Jou04].
- Identity-based cryptography [BF03].
- Short signature [BLS04].
- Self-blindable credential certificates [Ver01].
- Attribute based cryptography [SW05].
- Broadcast encryption [Goy+06].

Examples d'applications

Exemple (Diffie–Helman tripartite)

Alice envoie g^a, Bob envoie g^b, Charlie envoie g^c. La clé commune est

$$e(g,g)^{abc} = e(g^b,g^c)^a = e(g^c,g^a)^b = e(g^a,g^b)^c \in G_2.$$

Exemple (Signatures courtes)

- Clés : (P, sP), s. $s \in \mathbb{N}, P \in G_1$.
- Signature de M : $V = sM$.
- Vérification de V : $e(V,P) = e(M,sP)$.

Exemple (Cryptographie fondée sur l'identité)

- Clé maître : (P, sP), s. $s \in \mathbb{N}, P \in G_1$.
- Clé secondaire : Q, sQ. $Q \in G_1$.
- Chiffrement : $m \in G_2 : m' = m \oplus e(Q,sP)^r$, rP. $r \in \mathbb{N}$.
- Déchiffrement : $m = m' \oplus e(sQ,rP)$.

Examples d'applications

Exemple (Somewhat homomorphic encryption)

- Le chiffrement El-Gamal : $M \to (rP, M + rQ)$ est additif sur $E(\mathbb{F}_q)$ (r aléatoire) ;
- Donc le chiffrement dérivé : $m \in \mathbb{Z} \to (rP, mP + rQ)$ est additif sur $E(\mathbb{F}_q)$; on retrouve m à partir de mP par un DLP (temps $\sqrt{M}$ où M est le maximum des entiers pouvant être chiffrés) ;
- BGN05 [BGN05] : P est d'ordre $n = p_1 p_2$ un produit de grands nombres premiers, et on se donne Q un point d'ordre p_1.
- Le secret est p_1. Clé publique : P, Q, n.
- Chiffrement : $c = mP + rQ$ (r aléatoire dans $\mathbb{Z}/n\mathbb{Z}$). Déchiffrement : $p_2 c = m(p_2 P)$, que l'on retrouve par un DLP.
- $\mathrm{Add}(c_1, c_2) = c_1 + c_2 + rQ$.
- $\mathrm{Mult}(c_1, c_2) = e(c_1, c_2) \cdot e(Q, Q)^r$.
- Après une Mult on est dans μ_n. Le système reste additif (par rapport aux messages) et le déchiffrement est le DLP de c^{p_2} par rapport à $e(P, P)^{p_2}$.
- On peut donc évaluer n'importe quel polynôme quadratique à plusieurs variables directement sur les messages chiffrés !

Couplage de Weil sur les courbes elliptiques

- Soit $P, Q \in E[\ell]$ des points de ℓ-torsion ($\ell \neq p$).
- Rappel : $f_{\ell,P}$ a pour diviseur $\ell(P) - \ell(0)$.
- On définit
$$e_{W,\ell}(P,Q) = \frac{f_{\ell,P}((Q)-(0))}{f_{\ell,Q}((P)-(0))}.$$
- L'application $e_{W,\ell} : E[\ell] \times E[\ell] \to \mu_\ell$ est bilinéaire non dégénérée : c'est le couplage de Weil.

Définition (Embedding degree)

Si $E/\mathbb{F}_q$, on note d le plus petit entier tel que $\ell \mid q^d - 1$; autrement dit $\mathbb{F}_{q^d}$ est la plus petite extension contenant $\mu_\ell(\overline{\mathbb{F}_q})$.

Couplage de Weil sur les courbes elliptiques

Démonstration.

- $e_{W,\ell}(P,Q) = e_{W,\ell}(Q,P)^{-1}$ trivialement, donc il suffit de prouver la bilinéarité à droite ;
- $$\frac{f_{\ell,P}(Q+R)}{f_{\ell,Q+R}(P)} = \frac{f_{\ell,P}(Q)}{f_{\ell,Q}(P)}\frac{f_{\ell,P}(R)}{f_{\ell,R}(P)} \iff \frac{f_{\ell,P}(Q)f_{\ell,P}(R)}{f_{\ell,P}(Q+R)} = \frac{f_{\ell,Q}(P)f_{\ell,R}(P)}{f_{\ell,Q+R}(P)} \iff$$
$$f_{\ell,P}((Q)+(R)-(Q+R)-(0_E)) = \mu_{Q,R}^{\ell}((P)-(0_E))$$

  Comme $\mu_{Q,R}^{\ell}((P)-(0_E)) = \mu_{Q,R}(\ell(P)-\ell(0_E))$, l'égalité découle du théorème de réciprocité de Weil ;
- Le même genre d'argument montre que si $e_{W,\ell}(P,Q) = 1$ pour tout $Q \in E[\ell]$ alors il existerait $g_{\ell,P}$ tel que $f_{\ell,P} = g_{\ell,P}^{\ell}$, autrement dit $(P)-(0_E)$ serait principal, ce qui est absurde.

□

Couplage de Weil en pratique

- $E/\mathbb{F}_q$ courbe elliptique de cardinal $\#E(\mathbb{F}_q) = \ell$ premier ;
- Le polynôme caractéristique du Frobenius π agissant sur $E[\ell]$ est $X^2 - tX + q \mod \ell$;
- Si d est le degré de plongement et $d > 1$, alors $\pi = \left(\begin{smallmatrix} 1 & 0 \\ 0 & q \end{smallmatrix}\right)$ (car $q \neq 1 \mod \ell$).
- En particulier $E[\ell] \subset E(\mathbb{F}_{q^d})$ lorsque $d > 1$.
- On note $\mathbb{G}_1 = \mathrm{Ker}(\pi - \mathrm{Id})$ et $\mathbb{G}_2 = \mathrm{Ker}(\pi - q\,\mathrm{Id})$. $\mathbb{G}_1 = E[\ell](\mathbb{F}_q)$ et $\mathbb{G}_2 \subset E[\ell]$ est le sous-groupe de trace zero.
- Alors $e_{W,\ell}$ restreint à $\mathbb{G}_1 \times \mathbb{G}_2$ est non dégénérée.

Couplage de Tate sur $\mathbb{F}_q$

Définition

Le couplage de Tate est l'application bilinéaire non dégénérée :

$$\begin{array}{rcl} e_{T,\ell} : E_0[\ell](\mathbb{F}_q) \times E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) & \longrightarrow & \mathbb{F}_{q^d}^*/{\mathbb{F}_{q^d}^*}^\ell \\ (P,Q) & \longmapsto & f_{\ell,P}((Q)-(0)) \end{array} .$$

$$E_0[\ell] = \mathbb{G}_2 = \{P \in E[\ell](\mathbb{F}_{q^d}) \mid \pi(P) = [q]P\}.$$

- Sur $\mathbb{F}_{q^d}$ $(d>1)$, le couplage de Tate est un couplage

$$e_{T,\ell} : E[\ell](\mathbb{F}_{q^d}) \times E(\mathbb{F}_{q^d})/\ell E(\mathbb{F}_{q^d}) \to \mathbb{F}_{q^d}^*/{\mathbb{F}_{q^d}^*}^\ell \simeq \mu_\ell ;$$

- L'isomorphisme $\mathbb{F}_{q^d}^*/{\mathbb{F}_{q^d}^*}^\ell \simeq \mu_\ell$ est donné par $x \mapsto x^{(q^d-1)/\ell}$.
- Si $E(\mathbb{F}_{q^d})$ n'a pas de points de ℓ^2-torsion, alors $E(\mathbb{F}_{q^d})/\ell E(\mathbb{F}_{q^d}) \simeq E[\ell](\mathbb{F}_{q^d})$;
- Dans ce cas la restriction $e_{T,\ell} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_\ell$, $(P,Q) \mapsto f_{\ell,P}P(Q)^{(q^d-1)/\ell}$ est non dégénérée.

Preuve si $d > 1$

- Comme $E[\ell] \subset E(\mathbb{F}_{q^d})$, l'endomorphisme $\alpha = \frac{\pi^d - 1}{\ell}$ est bien défini : $\alpha(Q) = \pi^d(Q') - Q' \in E[\ell]$ où $\ell Q' = Q$.
- On peut montrer que $e_{T,\ell}(P,Q)^{(q^d-1)/\ell} = e_{W,\ell}(P, \alpha Q)$.
- Donc $e_{T,\ell}$ est bilinéaire. De plus l'image de α est isomorphe à $E(\mathbb{F}_{q^d})/\ell E(\mathbb{F}_{q^d})$, donc est de cardinal ℓ^2 donc α est surjective et $e_{T,\ell}$ est non dégénéré.
- α commute avec π donc stabilise $\mathbb{G}_1$ et $\mathbb{G}_2$ donc la restriction de $e_{T,\ell}$ a $\mathbb{G}_1 \times \mathbb{G}_2$ est non dégénérée. (Quand $E(\mathbb{F}_{q^d})$ n'a pas de points de ℓ^2-torsion.)

- Si $d = 1$, alors $\alpha : E(\mathbb{F}_q)/\ell E(\mathbb{F}_q) \to H^1(G, E[\ell]) \simeq E[\ell]/(\pi - 1)$, et $e_{W,\ell}(P, \alpha Q) \in H^1(G, \mu_\ell) \simeq \mathbb{F}_q^*/\mathbb{F}_q^{*\ell} \simeq \mu_\ell/(\pi - 1) = \mu_\ell$ où G est le groupe de Galois de $\mathbb{F}_q$.
- Le couplage de Tate reste bien défini et non dégénéré. Si $\mathbb{G}_1$ est cyclique engendré par P, $e_{T,\ell}(P,P) \neq 1$.

Élimination des dénominateurs

- On suppose $d > 1$ pair ;
- Si $P \in \mathbb{G}_1$, $x_P \in \mathbb{F}_q$;
- si $Q \in \mathbb{G}_2$ alors $x_Q \in \mathbb{F}_{q^{k/2}}$.
- En effet $q^{k/2} = -1 \mod \ell$ donc $\pi^{q^{k/2}}(Q) = -Q$.
- Donc si $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ alors le dénominateur de $f_P(Q)$ vit dans $\mathbb{F}_{q^{k/2}}$, donc il sera tué par l'exponentiation finale par $(q^d - 1)/\ell$.
- Pas besoin de s'embêter à calculer les dénominateurs $v_{\lambda P}(Q)$!

Miller's algorithm on elliptic curves

Algorithme (Computing the Tate pairing)

Input: $\ell \in \mathbb{N}$, $P = (x_1, y_1) \in E[\ell](\mathbb{F}_q)$, $Q = (x_2, y_2) \in E(\mathbb{F}_{q^d})$, d even.

Output: $e_T(P, Q)$.

1. *Compute the binary decomposition :* $\ell := \sum_{i=0}^{l} b_i 2^i$. *Let* $T = P, f_1 = 1, f_2 = 1$.
2. *For* i *in* $[l \,..0]$ *compute*
   1. α, *the slope of the tangent of* E *at* T.
   2. $T = 2T$. $T = (x_3, y_3)$.
   3. $f_1 = f_1^2(y_2 - \alpha(x_2 - x_3) - y_3)$, $f_2 = f_2^2(x_2 + (x_1 + x_3) - \alpha^2)$.
   4. *If* $b_i = 1$, *then compute*
      1. α, *the slope of the line going through* P *and* T.
      2. $T = T + Q$. $T = (x_3, y_3)$.
      3. $f_1 = f_1^2(y_2 - \alpha(x_2 - x_3) - y_3)$, $f_2 = f_2(x_2 + (x_1 + x_3) - \alpha^2)$.

Return

$$\left(\frac{f_1}{f_2}\right)^{\frac{q^d - 1}{\ell}}.$$

Bibliography

D. Boneh et M. Franklin. « Identity-based encryption from the Weil pairing ». In : *SIAM Journal on Computing* 32.3 (2003), p. 586–615 (cf. p. 34).

D. Boneh, B. Lynn et H. Shacham. « Short signatures from the Weil pairing ». In : *Journal of Cryptology* 17.4 (2004), p. 297–319 (cf. p. 34).

D. Boneh, E.-J. Goh et K. Nissim. « Evaluating 2-DNF Formulas on Ciphertexts. ». In : *TCC*. T.3378. Springer. 2005, p. 325–341 (cf. p. 36).

V. Goyal, O. Pandey, A. Sahai et B. Waters. « Attribute-based encryption for fine-grained access control of encrypted data ». In : *Proceedings of the 13th ACM conference on Computer and communications security*. ACM. 2006, p. 98 (cf. p. 34).

A. Joux. « A one round protocol for tripartite Diffie–Hellman ». In : *Journal of Cryptology* 17.4 (2004), p. 263–276 (cf. p. 34).

A. Sahai et B. Waters. « Fuzzy identity-based encryption ». In : *Advances in Cryptology–EUROCRYPT 2005* (2005), p. 457–473 (cf. p. 34).

E. Verheul. « Self-blindable credential certificates from the Weil pairing ». In : *Advances in Cryptology—ASIACRYPT 2001* (2001), p. 533–551 (cf. p. 34).