Utilisation des (hyper)elliptic nets en cryptographie

Christophe Tran

IRMAR, Université de Rennes 1

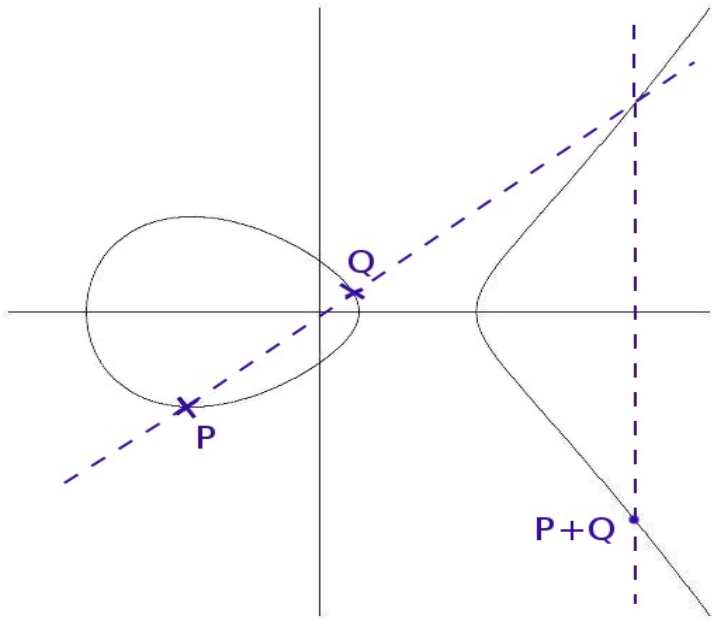
Couplages cryptographiques

Définition

Soient $\mathbb{G}_1$, $\mathbb{G}_2$ et $\mathbb{G}_T$ des groupes de "taille cryptographique".
Un couplage est une fonction $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ bilinéaire non dégénérée.
Dans cet exposé, on va s'intéresser au calcul du **couplage de Tate**.

Loi de groupe sur une courbe elliptique

Soit $\mathcal{E}/\mathbb{F}_q$ une courbe elliptique.



$$[n]P = \underbrace{P + \cdots + P}_{n \text{ fois}}, \ \mathcal{E}[n] = \{P \in \mathcal{E} \mid [n]P = \mathcal{O}\}.$$

Couplage de Tate

Définition (Fonctions de Miller)

$P \in \mathcal{E}[r]$, $i \in \mathbb{N}$: $(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O})$.

$$e(P, Q) = f_{r,P}(Q).$$

Polynômes de division

Définition (Polynômes de division)

$i \in \mathbb{N}$, $A \in \mathcal{E}$,

$$[i]A = \mathcal{O} \Leftrightarrow \Psi_i(A) = 0.$$

- $(\Psi_i) = [i]^*\mathcal{O} - i^2(\mathcal{O})$
- $\left(\frac{\Psi_{i+j}\Psi_{i-j}}{\Psi_i^2\Psi_j^2}\right) = [i+j]^*\mathcal{O} + [i-j]^*\mathcal{O} - 2[i]^*\mathcal{O} - 2[j]^*\mathcal{O}$

$$\Rightarrow \frac{\Psi_{i+j}(P)\Psi_{i-j}(P)}{\Psi_i(P)^2\Psi_j(P)^2} = x_{[i]P} - x_{[j]P}.$$

Retour sur les fonctions de Miller

- $F : (P, Q) \mapsto \frac{f_{i+j,P}(Q) f_{i-j,P}(Q)}{f_{i,P}(Q)^2 \Psi_j(P)^2} \in \mathbb{F}_q[\mathcal{E} \times \mathcal{E}]$
- $Q \mapsto F(P, Q)$ a pour diviseur

$$([i+j]P) + ([i-j]P) - 2([i]P)$$

$$\Rightarrow \frac{f_{i+j,P}(Q) f_{i-j,P}(Q)}{f_{i,P}(Q)^2 \Psi_j(P)^2} = x_{Q+[i]P} - x_{[j]P}.$$

Généralisation : les elliptic nets(1)

Définition

$a, b \in \mathbb{Z},\ P, Q \in \mathcal{E},$

$$[a]P + [b]Q = \mathcal{O} \Leftrightarrow W_{a,b}(P, Q) = 0$$

Exemples :

- $b = 0 : W_{a,0}(P, Q) = \Psi_a(P)$
- $b = 1 : W_{a,1}(P, Q) = f_{a,P}(Q)$

Généralisation : les elliptic nets(2)

Proposition

$a, b, c, d \in \mathbb{Z}$,

$$\frac{W_{a+b,c+d}(P,Q)W_{a-b,c-d}(P,Q)}{W_{a,c}(P,Q)^2 W_{b,d}(P,Q)^2} = x_{[a]P+[c]Q} - x_{[b]P+[d]Q}.$$

Démonstration.

$P \mapsto \frac{W_{a+b,c+d}(P,Q)W_{a-b,c-d}(P,Q)}{W_{a,c}(P,Q)^2 W_{b,d}(P,Q)^2}$ a pour diviseur

$$[a+b]^*([-c-d]Q)+[a-b]^*([d-c]Q)-2[a]^*([-c]Q)-2[b]^*([-d]Q)$$

Désormais, on fixe $P, Q \in \mathcal{E}$, et on voit W comme une fonction sur $\mathbb{Z}^2$. W est appelée *elliptic net* associée à P et Q.
On veut donc calculer $W(r, 1)$.

Récurrence des elliptics nets

Théorème

Pour tout $\mathfrak{u}, \mathfrak{v}, \mathfrak{s}, \mathfrak{t} \in \mathbb{Z}^2$,

$$\begin{aligned} &W(\mathfrak{u}+\mathfrak{v})W(\mathfrak{u}-\mathfrak{v})W(\mathfrak{s}+\mathfrak{t})W(\mathfrak{s}-\mathfrak{t}) \\ &\quad + W(\mathfrak{u}+\mathfrak{s})W(\mathfrak{u}-\mathfrak{s})W(\mathfrak{t}+\mathfrak{v})W(\mathfrak{t}-\mathfrak{v}) \\ &\quad + W(\mathfrak{u}+\mathfrak{t})W(\mathfrak{u}-\mathfrak{t})W(\mathfrak{v}+\mathfrak{s})W(\mathfrak{v}-\mathfrak{s}) = 0 \end{aligned}$$

Récurrence des elliptics nets : preuve(1)

Notation : $\mathfrak{a} = (a_1, a_2) \in \mathbb{Z}^2$, $\mathfrak{P} = (P_1, P_2) \in \mathcal{E}^2$,

$$[\mathfrak{a}].\mathfrak{P} = [a_1]P_1 + [a_2]P_2.$$

$$\frac{W(\mathfrak{u}+\mathfrak{v})W(\mathfrak{u}-\mathfrak{v})W(\mathfrak{s}+\mathfrak{t})W(\mathfrak{s}-\mathfrak{t})}{W(\mathfrak{u})^2W(\mathfrak{v})^2W(\mathfrak{s})^2W(\mathfrak{t})^2} = \left(x_{[\mathfrak{u}].\mathfrak{P}} - x_{[\mathfrak{v}].\mathfrak{P}}\right)\left(x_{[\mathfrak{s}].\mathfrak{P}} - x_{[\mathfrak{t}].\mathfrak{P}}\right)$$

$$\frac{W(\mathfrak{u}+\mathfrak{s})W(\mathfrak{u}-\mathfrak{s})W(\mathfrak{t}+\mathfrak{v})W(\mathfrak{t}-\mathfrak{v})}{W(\mathfrak{u})^2W(\mathfrak{v})^2W(\mathfrak{s})^2W(\mathfrak{t})^2} = \left(x_{[\mathfrak{u}].\mathfrak{P}} - x_{[\mathfrak{s}].\mathfrak{P}}\right)\left(x_{[\mathfrak{t}].\mathfrak{P}} - x_{[\mathfrak{v}].\mathfrak{P}}\right)$$

$$\frac{W(\mathfrak{u}+\mathfrak{t})W(\mathfrak{u}-\mathfrak{t})W(\mathfrak{v}+\mathfrak{s})W(\mathfrak{v}-\mathfrak{s})}{W(\mathfrak{u})^2W(\mathfrak{v})^2W(\mathfrak{s})^2W(\mathfrak{t})^2} = \left(x_{[\mathfrak{u}].\mathfrak{P}} - x_{[\mathfrak{t}].\mathfrak{P}}\right)\left(x_{[\mathfrak{v}].\mathfrak{P}} - x_{[\mathfrak{s}].\mathfrak{P}}\right)$$

Récurrence des elliptics nets : preuve(2)

$P_1 \mapsto \frac{W(\mathfrak{u}+\mathfrak{v})W(\mathfrak{u}-\mathfrak{v})}{W(\mathfrak{u})^2 W(\mathfrak{v})^2} \in \mathcal{L}(2([u_2]P_2))$ qui est un e.v. de dim 2.

$$\Rightarrow det\left(\frac{W(\mathfrak{u}_i+\mathfrak{u}_j)W(\mathfrak{u}_i-\mathfrak{u}_j)}{W(\mathfrak{u}_i)^2 W(\mathfrak{u}_j)^2}\right)_{1\leq i,j\leq 4} = 0.$$

$$\Rightarrow det\left(W(\mathfrak{u}_i+\mathfrak{u}_j)W(\mathfrak{u}_i-\mathfrak{u}_j)\right)_{1\leq i,j\leq 4} = 0.$$

Applications

$$
\begin{aligned}
W(2i-1,0) &= W(i+1,0)W(i-1,0)^3 - W(i-2,0)W(i,0)^3, \\
W(2i,0)W(2,0) &= W(i,0)W(i+2,0)W(i-1,0)^2 \\
&\quad - W(i,0)W(i-2,0)W(i+1,0)^2, \\
W(2i-1,1)W(1,1) &= W(i-1,1)W(i+1,1)W(i-1,0)^2 \\
&\quad - W(i,0)W(i-2,0)W(i,1)^2, \\
W(2i,1) &= W(i-1,1)W(i+1,1)W(i,0)^2 \\
&\quad - W(i-1,0)W(i+1,0)W(i,1)^2.
\end{aligned}
$$

Remarques finales

- La démonstration de la relation des elliptic nets n'utilise pas le modèle de la courbe.
- La notion d'elliptic nets se généralise au cas hyperelliptique : $dim(\mathcal{L}(2.X)) = 2^g$.

Merci de votre attention