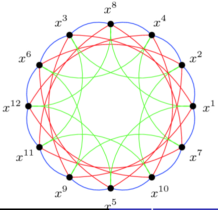
Implémentation du protocole CRS d'échange de clefs à base d'isogénies

Hugo Nartz, Clément Jacquot

16 Février 2022



Paramètres globaux

Corps de base:

$$\mathbb{F}_p \text{ avec } p \sim 2^{512}.$$

Courbe de base avec de bonnes propriétés:

$$E : Y^2 = X^3 + AX^2 + X \text{ où } A \in \mathbb{F}_p.$$

Notamment $\#E(\mathbb{F}_p) = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdots$

Isogénies et Frobenius

- l: petit diviseur premier de $\#E(\mathbb{F}_p)$ co-premier à p.
- Pour tout $P \in E(\mathbb{F}_p)[l]$ il existe une unique l-isogénie

  $$\phi : E \to E/ < P >$$

  telle que $\ker \phi =< P >$.
- Pour certains l (*Elkies primes*), le Frobenius

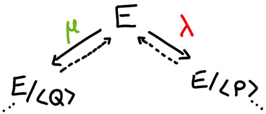
  $$\pi : (x, y) \in E[l] \mapsto (x^p, y^p) \in E[l]$$

  a deux valeurs propres λ et μ.
- $E[l]$ est somme de deux sous-espaces propres de cardinaux l: deux isogénies associées.

Graphes d'isogénies

- Deux l-isogénies par courbe: deux directions (λ et μ).
- Isogénie *duale* de degré l ($\dashrightarrow$): pour revenir en arrière.
- Conservation des propriétés dans la composante connexe

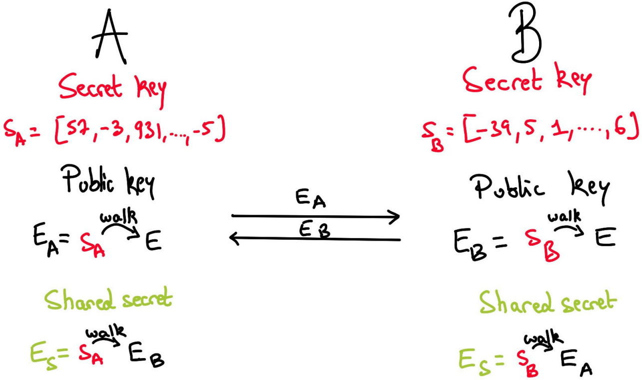
$\rightarrow$ Pour chaque l (Elkies): un cycle dont les sommets sont des courbes elliptiques et les arêtes des isogénies.



$\rightarrow$ Les pas dans le graphe commutent par rapport aux differents l.

L'échange de clefs

- Clef privée s: nombre de pas (aléatoire) pour chaque l.
- Clef publique: marche suivant les pas de la clef secrète $s \curvearrowright E$.



Points de l-torsion

On cherche $P \in E(\mathbb{F}_q)[l] = \ker \phi$. Posons $C = \#E(\mathbb{F}_q)/l$.

- Soit $Q \in E(\mathbb{F}_q)$ aléatoire.
- Si $P := C \cdot Q \neq O$, on a gagné.
- Sinon on tire un autre Q.

Si $\#E(\mathbb{F}_q) = l \cdot p_1^{f_1} \cdots p_n^{f_n}$ avec $l \wedge p_i = 1$,

$$Q = (e_0, e_1, \cdots, e_n) \in \mathbb{Z}_l \times \mathbb{Z}_{p_1^{f_1}} \times \mathbb{Z}_{p_n^{f_n}},$$
$$C \cdot Q = (\kappa e_0, 0, \cdots, 0) \text{ pour } \kappa \in \mathbb{F}_l^*.$$

Le point $C \cdot Q$ convient avec probabilité $1 - 1/l$.

Arithmétique de Montgomery

- Courbe de Montgomery $E_{A,B} : By^2 = x^3 + Ax^2 + x$
- $\mathbf{x}\colon (X : Y : Z) \in E_{A,B} \mapsto (X : Z) \in \mathbb{P}^1$
- La loi de $E_{A,B}$ induit par $\mathbf{x}$ une loi sur $\mathbb{P}^1$

Prop. $P, Q \in E$

Si $P \neq Q$ alors

$$\begin{cases} X_{P+Q} = Z_{P-Q}[(X_P - Z_P)(X_Q + Z_Q) + (X_P + Z_P)(X_Q - Z_Q)]^2 \\ Z_{P+Q} = X_{P-Q}[(X_P - Z_P)(X_Q + Z_Q) - (X_P + Z_P)(X_Q - Z_Q)]^2 \end{cases}$$

Si $P = Q$ alors

$$\begin{cases} X_{[2]P} = (X_P + Z_P)^2(X_P - Z_P)^2 \\ Z_{[2]P} = (4X_PZ_P)[(X_P - Z_P)^2 + \frac{A+2}{4}(4X_PZ_P)] \end{cases}$$

Arithmétique de Montgomery

- Courbe de Montgomery $E_{A,B} : By^2 = x^3 + Ax^2 + x$
- $\mathbf{x}$: $(X : Y : Z) \in E_{A,B} \mapsto (X : Z) \in \mathbb{P}^1$
- La loi de $E_{A,B}$ induit par $\mathbf{x}$ une loi sur $\mathbb{P}^1$
- On remote à $E_{A,B}$ en remarquant que $\mathbf{x}(P) = \mathbf{x}(Q) \Leftrightarrow P = \pm Q$
- $\mathbf{x}(P) + \mathbf{x}(Q)$ détermine $\{\mathbf{x}(P \pm Q)\}$
- xADD : $(\mathbf{x}(P), \mathbf{x}(Q), \mathbf{x}(P - Q)) \mapsto \mathbf{x}(P + Q)$
- xDBL : $\mathbf{x}(P) \mapsto \mathbf{x}(2P)$

Montgomery Ladder pseudocode

Entrées : $P, k = \sum_{i=0}^{l-1} k_i 2^i$ avec $k_{l-1} = 1$
Sortie : kP

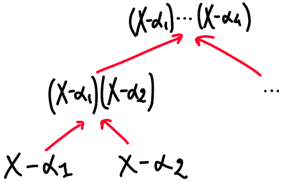
```
P0 = P
P1 = xDBL(P)
for(int i=l-2; i>=0, i--) {
  if(k[i]==0){
    P1 = xADD(P0, P1, P)
    P0 = xDBL(P0)
  }
  else{
    P0 = xADD(P0, P1, P)
    P1 = xDBL(P1)
  }
}
return P0
```

Invariants: $P1 = P0 + P$ et après i itérations, $\begin{array}{l} P0 = \lfloor k/2^i \rfloor P \\ P1 = \lfloor k/2^i + 1 \rfloor P \end{array}$

Multi-evaluation

- Problème: évaluer $P \in \mathbb{F}_q[X]$ en $\alpha_1, \cdots, \alpha_n$.
- Equivalent à $P \bmod (X - \alpha_i)$.

Exemple pour $n = 4$: on construit par le bas



Puis on réduit P en descendant.
Complexité: $\mathbf{M}(n) \log n$ si $\deg(P) \sim n$.