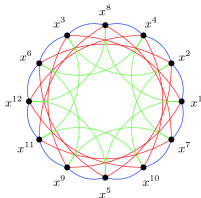


# Implémentation du protocole CRS d'échange de clefs à base d'isogénies

Hugo Nartz, Clément Jacquot

16 Février 2022



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

# 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

$$\phi : E \rightarrow E / \langle P \rangle$$

telle que  $\ker \phi = \langle P \rangle$ .

- Pour certains  $l$  (*Elkies primes*), le Frobenius

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

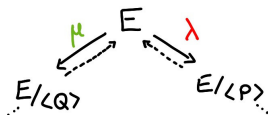
a deux valeurs propres  $\lambda$  et  $\mu$ .

- $E[l]$  est somme de deux sous-espaces propres de cardinaux  $l$ : deux isogénies associées.

# Graphes d'isogénies

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

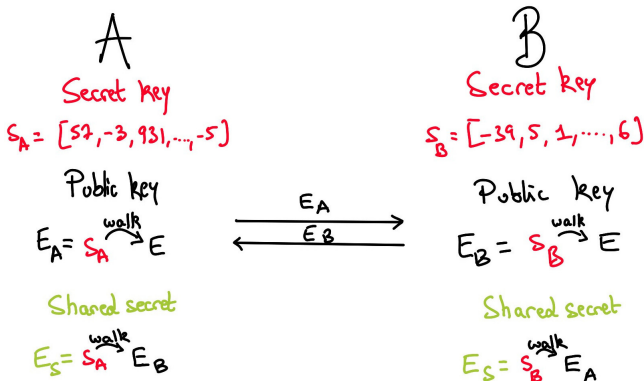
→ Pour chaque  $l$  (Elkies): un cycle dont les sommets sont des courbes elliptiques et les arêtes des isogénies.



→ Les pas dans le graphe commutent par rapport aux différents  $l$ .

# 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  $l \wedge p_i = 1$ ,

$$Q = (e_0, e_1) \in \mathbb{Z}_l \times G, \quad G \text{ abélien et } \#G = C,$$
$$C \cdot Q = (\kappa e_0, 0) \text{ pour } \kappa \in \mathbb{F}_l^*.$$

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

- 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  $\mathbb{P}^1$

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

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

# 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 remonte à  $E_{A,B}$  en remarquant que
$$\mathbf{x}(P) = \mathbf{x}(Q) \Leftrightarrow P = \pm Q$$
- $\mathbf{x}(P) \pm \mathbf{x}(Q)$  détermine  $\{\mathbf{x}(P \pm Q)\}$
- $\mathbf{xADD} : (\mathbf{x}(P), \mathbf{x}(Q), \mathbf{x}(P - Q)) \mapsto \mathbf{x}(P + Q)$
- $\mathbf{xDBL} : \mathbf{x}(P) \mapsto \mathbf{x}(2P)$



# Pseudo-code échelle de Montgomery

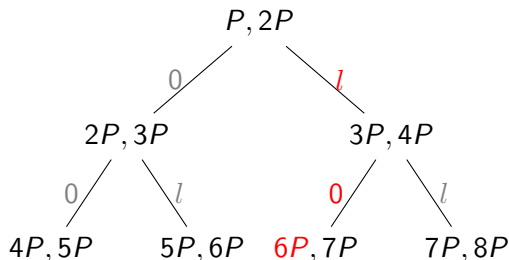
Entrées :  $P, k = \sum_{i=0}^{l-1} k_i 2^i$  avec  $k_{l-1} = 1$

Sortie :  $kP$

```
1  P0 = P
2  P1 = xDBL(P)
3  for(int i=l-2; i>=0, i--) {
4      if(k[i]==0){
5          P1 = xADD(P0, P1, P)
6          P0 = xDBL(P0)
7      }
8      else{
9          P0 = xADD(P0, P1, P)
10         P1 = xDBL(P1)
11     }
12 }
13 return P0
```

# Échelle de Montgomery

**Exemple.**  $k = 6 = \overline{110}^2$



**Invariants:**  $P1 = P0 + P$  et,

après  $r$  iterations,  $i = l - 2 - r$ ,  
 $P0 = \lfloor k/2^i \rfloor P$   
 $P1 = \lfloor k/2^i + 1 \rfloor P$

## 2 méthodes

- Pour  $l \in \{3, 5, 7\}$ : formules radicales.
- Pour  $l \in \{11, 13, \dots, 1723\}$ :  $\sqrt{-}$ Vélu.

- Donnée : un point  $P$  de  $l$ -torsion.
- But : effectuer un pas sur le graphe d'isogénies.

**Prop.**  $\phi : E_A \rightarrow E_{A'}$  isogénie de noyau  $\langle P \rangle$ .

On a alors  $A' = 2 \frac{1+d}{1-d}$  où

$$d = \left( \frac{A-2}{A+2} \right)^l \left( \frac{h_S(1)}{h_S(-1)} \right)^8, \text{ et}$$

$$h_S(X) = \prod_{s \in S} (X - \mathbf{x}([s]P)), \text{ avec } S = \{1, 3, \dots, l-2\}$$

- $h_S(X) = \prod_{s \in S} (X - \mathbf{x}([s]P))$ , avec  $S = \{1, 3, \dots, l-2\}$

Idée. Ecrire  $S = (I \pm J) \cup K$  avec  $\sqrt{l/2} \simeq \#I \simeq \#J \simeq \#K$

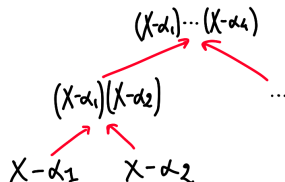
- $h_{I \pm J} = h_{I+J} h_{I-J}$
- $\mathbf{x}(P), \mathbf{x}(Q), \mathbf{x}(P+Q), \mathbf{x}(P-Q)$  sont fondamentalement reliés.
- On exprime  $h_{I \pm J} = \text{Res}(h_I, R_J)$  où  $R_J \in \mathbb{F}_p[X]$
- Les racines de  $h_I$  étant connues, ce calcul se ramène à une multi-évaluation

$$\text{Res}(h_I, R_J) = \prod_{i \in I} R_J(\mathbf{x}([i]P))$$

# Multi-évaluation

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

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



Puis on réduit  $P$  en descendant.

Complexité:  $O(\mathbf{M}(n) \log n)$  si  $\deg(P) \sim n$ .

# Isogénies radicales

- Pour  $l \in \{3, 5, 7\}$  .
- Model:  $F = y^2 + (1 - c)xy - by - x^2(x - b)$ .

On cherche des chaines de  $l$ -isogénies (ici  $k$ -pas)

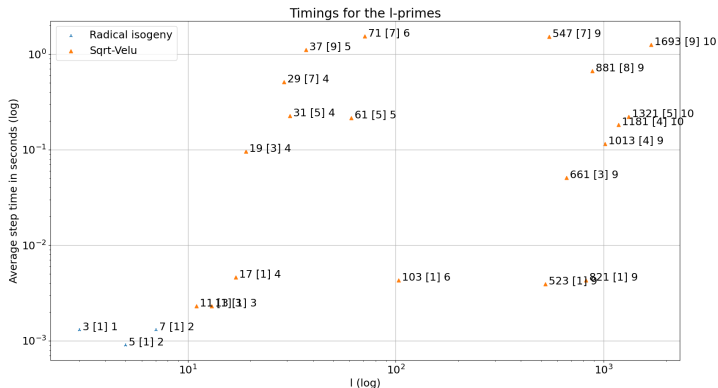
$$E \rightarrow E_1 \rightarrow E_2 \rightarrow \cdots \rightarrow E_{k-1} \rightarrow E_k.$$

Exemple d'un pas ( $l = 5$ ):

$$b' = \alpha \frac{\alpha^4 + 3\alpha^3 + 4\alpha^2 + 2\alpha + 1}{\alpha^4 - 3\alpha^3 + 4\alpha^2 - 2\alpha + 1}$$

Pour  $\alpha = \sqrt[5]{b}$ .

Clef la plus lente: 270 secondes (échange en 540s).





- Code vérifié avec Valgrind.
- 25% plus rapide que l'implémentation précédente, 92% par rapport à l'article de 2018.

Mais

- Deux premiers  $l$  inutilisables ( $\sim 10$  bits).
- Structures trop rigides.

Optimisations potentielles:

- Parallélisation GPU/multi-threading pour la multi-évaluation.
- Plus de caching.
- Plus de formules radicales.
- Meilleure courbe de base.

# Formules d'additions affine

Soient  $P = (x_P, y_P)$ ,  $Q = (x_Q, y_Q) \in E_{A,B}$  avec  $x_P \neq x_Q$  et  $x_P x_Q \neq 0$ .  
Notons  $P + Q = (x_{P+Q}, y_{P+Q})$  et  $P - Q = (x_{P-Q}, y_{P-Q})$ . Alors  $x_{P+Q}$  satisfait

$$\begin{aligned}x_{P+Q} &= B[(y_P - y_Q)/(x_P - x_Q)]^2 - A - x_P - x_Q \\&= \frac{1}{(x_P - x_Q)^2} (B(y_P - y_Q)^2 - (A + x_P + x_Q)(x_P - x_Q)^2) \\&= \frac{1}{(x_P - x_Q)^2} (-2B y_P y_Q + x_P x_Q (x_P + x_Q + 2A) + x_P + x_Q) \\&= \frac{B(x_Q y_P - x_P y_Q)^2}{x_P x_Q (x_P - x_Q)^2}\end{aligned}$$

De même,  $x_{P-Q} = \frac{B(x_Q y_P + x_P y_Q)^2}{x_P x_Q (x_P - x_Q)^2}$

En multipliant ces équations, on obtient

$$x_{P+Q} x_{P-Q} (x_P - x_Q)^2 = (x_P x_Q - 1)^2$$

# Formules d'additions projectives

On passe en coordonnées projectives. En écrivant les quotients  $x = X/Z$  pour chaque point en question, On vérifie alors que  $\mathbf{x}(P + Q) = (X_{P+Q} : Z_{P+Q})$  avec

$$X_{P+Q} = Z_{P-Q}(X_P X_Q - Z_P Z_Q)^2$$

$$Z_{P+Q} = X_{P-Q}(X_P Z_Q - Z_P X_Q)^2$$

Ces formules nécessitent 8 multiplications mais peuvent être réécrites en

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

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

qui ne nécessitent plus que 6 multiplications.

- $l \in \{3, 5, 7\}$ .
- $p + 1 = 0 \pmod{2l}$ .
- On écrit  $p + 1 = 2/k$  pour un certain  $k$ .
- Il vient  $(x^k)^l = \pm x$ .