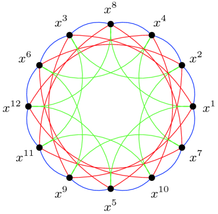
Implémentation du protocole CRS d'échange de clefs à base d'isogénies

Hugo Nartz, Clément Jacquot

16 Février 2022



1. Le protocol CRS
   - Conclusion

Paramètres de base

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

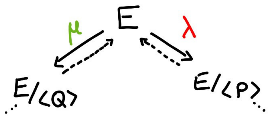
$$\pi : (x, y) \in E[l] \mapsto (x^p, y^p) \in E[l]$$

  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 $s \curvearrowright E$.