Implementation of the isogeny-based key-exchange protocol CRS

Hugo Nartz, Clément Jacquot

February 16, 2022

Définitions et permier résultat

Algorithme des fractions continues

Fraction rationelle

- $n \in \mathbb{N}$
- $X_0, X_1, \ldots, X_n$ des variables
- $F_0 = X_0$
- $F_{n+1}(X_0, \cdots, X_{n+1}) = F_n(X_0, \cdots, X_n + \frac{1}{X_{n+1}})$
- Notation: $F_n = [X_0, \cdots, X_n]$

Réduite et quotients

-

Proposition

- Il existe deux suites (P_n) et (Q_n) de polynomes tels que:
- P_n et Q_n ne dépendent que de $X_0, \cdots, X_n$
- $P_0 = X_0, P_1 = X_0X_1 + 1$ et $Q_0 = 1, Q_1 = X_1$
- $\forall n \geq 2 : P_n = X_nP_{n-1} + P_{n-2}$ et $Q_n = X_nQ_{n-1} + Q_{n-2}$

Théorème

- $\forall n \geq 0$
- $F_n = [X_0, \cdots, X_n] = \frac{P_n}{Q_n}$

Algorithme

- $\theta \in \mathbb{R}$
- $a_0 = [\theta]$
- Si $\theta \in \mathbb{Z}$ alors $\theta = a_0$ fin
- Sinon $\theta - a_0 \in]0, 1[$ et il existe θ_1 tel que $\theta = a_0 + \frac{1}{\theta_1}$, on réitère le processur pour $\theta = \theta_1$ et $a_1 = [\theta_1]$
- L'algorithme termine si et seulement si il existe n tel que $\theta_n = [a_n]$