Gaël Le Mahec

Sorina Ionica
Gilles Dequen

Une nouvelle approche pour la résolution parallèle du logarithme discret

Monika Trimoska

Cryptographie à clé publique

Le problème du logarithme discret

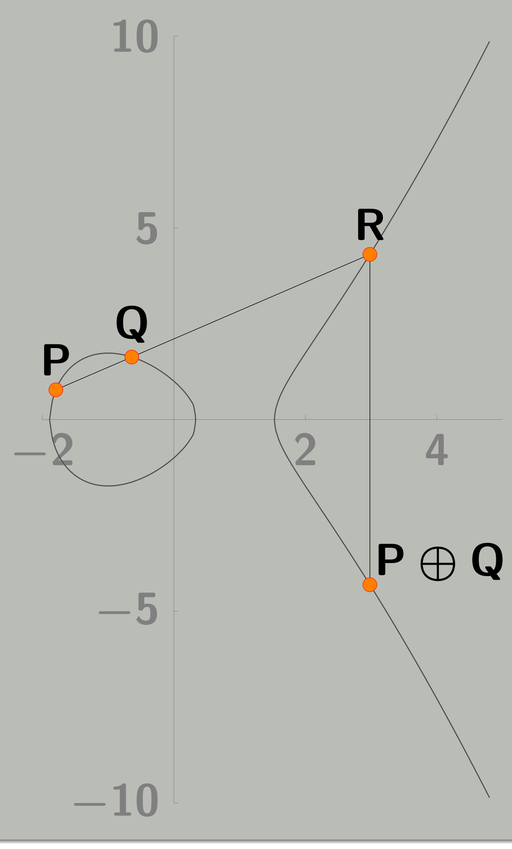
$$g^x = h \pmod p$$

Cryptographie à base de courbes elliptiques

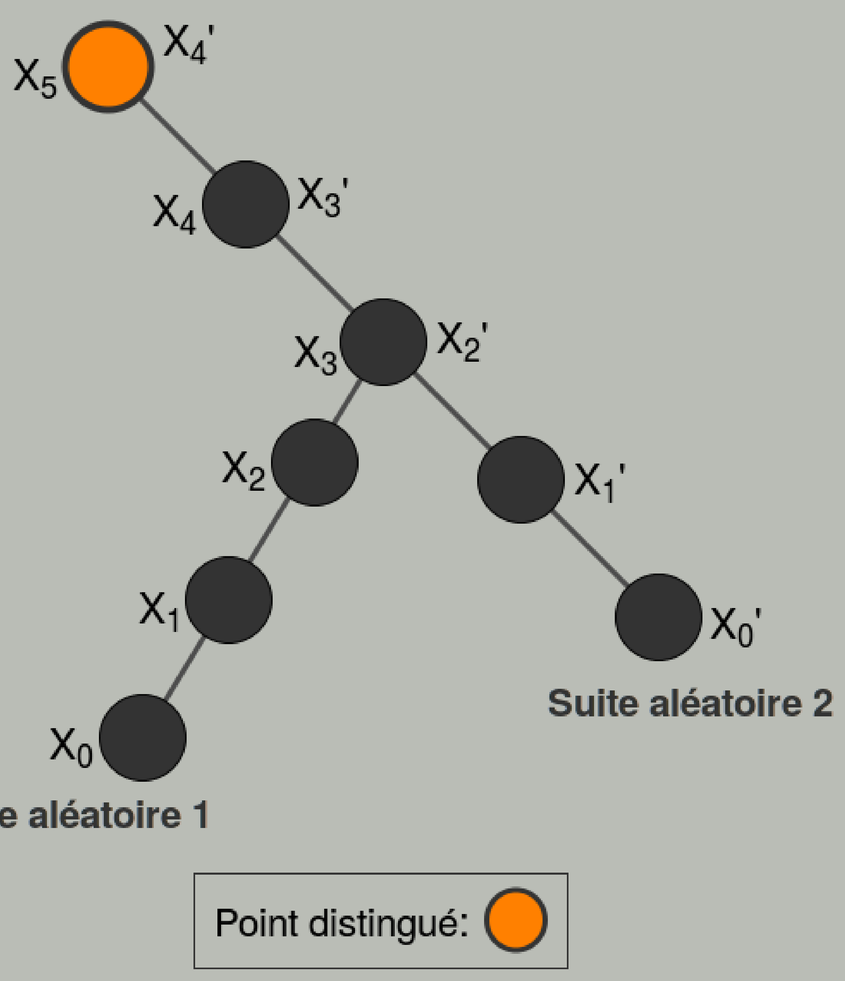
Une courbe définie par l'équation

$$y^2 = x^3 + Ax + B \pmod p,$$

munie d'une addition géométrique sur ses points.



Recherche de collision



- Chaque thread calcule une suite aléatoire de points
- Uniquement les points distingués sont stockés
- Collision: le logarithme discret $\mathbf{Q = xP}$ est résolu

Mémoire : Arbre radix

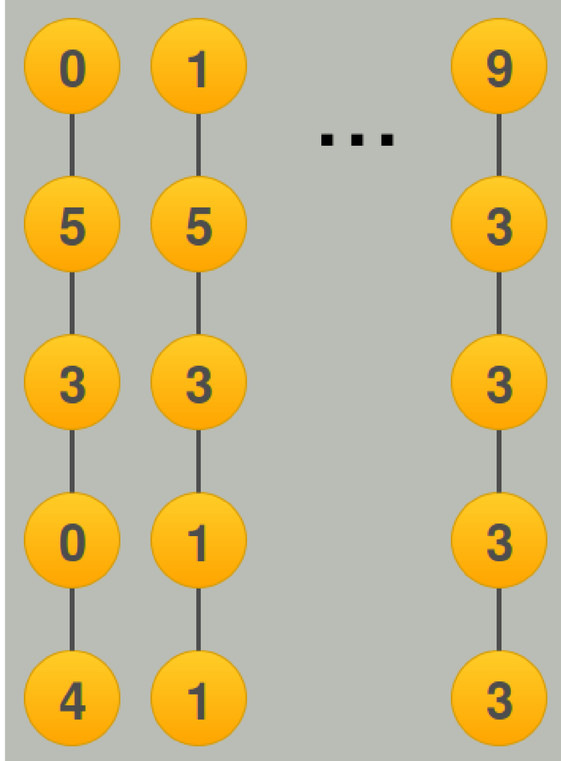


Figure : 10 points stockés - pire des cas

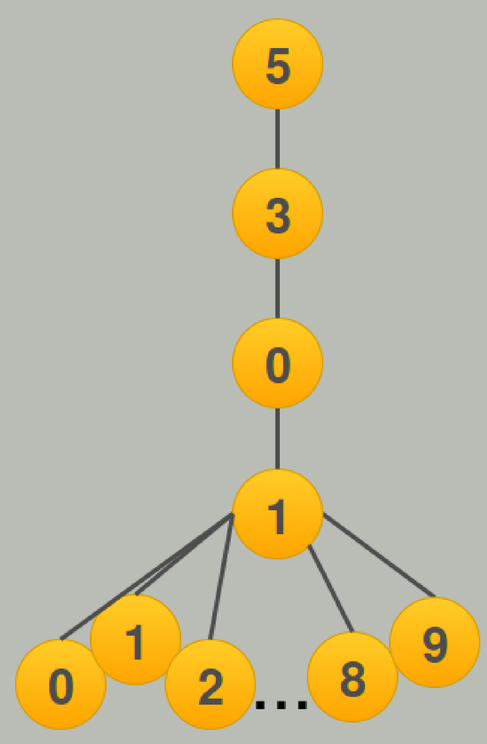
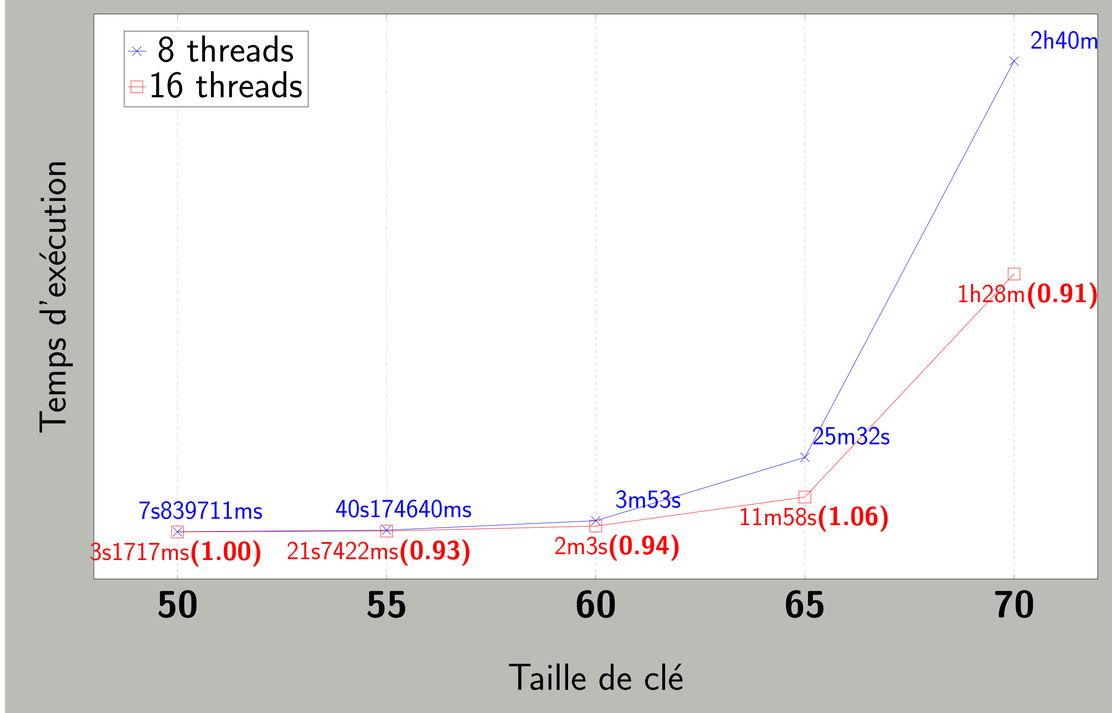


Figure : 10 points stockés - meilleur des cas

- Optimisation de la mémoire
- La recherche et l'insertion d'un point est une seule opération - $\mathbf{O(log(n))}$
- Probabilité d'attente de verrouillage très faible

Performance parallèle

Comparaison de temps d'exécution de Parallel Collision Search



Pour des clés de taille $\geq$ 50 bits, la performance parallèle est linéaire.

Complexité théorique

Complexité en temps de notre algorithme

$$(\frac{1}{L}\sqrt{\frac{\pi n}{2}} + \frac{1}{\theta})t_c + (\frac{\theta}{L}\sqrt{\frac{\pi n}{2}})t_s$$

- $\mathbf{L}$ - nombre de threads
- $\mathbf{n}$ - nombre de points de la courbe
- θ - probabilité qu'un point soit distingué
- $\mathbf{t_c}$ et $\mathbf{t_s}$ - constantes