Cryptographie basée sur les courbes elliptiques

Une introduction en images

Félix Larose-Gervais

Plan de l’exposé

- Définitions
  - Courbes elliptiques
  - Structure de groupe des points
  - Algorithme de multiplication rapide par addition et doublement
  - Problème du logarithme discret
- Applications
  - **Confidentialité**: Échange de clés Diffie-Hellman
  - **Authenticité**: Algorithme de Signature Digitale