



Algorithme de Signature Digitale (ECDSA)

Les grandes lignes

- Soient une courbe \mathcal{C} sur \mathbb{F}_p et $P \in \mathcal{C}$ tel que $|\langle P \rangle| = n$ (p, n premiers)
- Alice choisi $a \in \mathbb{F}_p$ sa clé privée et calcule $A = aP \in \mathcal{C}$ sa clé publique
- Pour signer le message m , Alice
 - Choisi un $k \in \mathbb{F}_n$ aléatoire, calcule $e \in \mathbb{F}_n$ le hash tronqué de m et le point $(x, y) = kP$
 - Calcule la signature $(r, s) \equiv (x, k^{-1}(e + ra)) \pmod{n}$
- Pour vérifier la signature (r, s) du message m , Bob
 - Calcule $(u, v) \equiv (es^{-1}, rs^{-1}) \pmod{n}$
 - Vérifie que le point $uP + vA = \mathcal{O}$