

Échange de clé Diffie-Hellman (ECDH)

Sur la courbe 25519

- Soit $p = 2^{255} - 19$, la courbe $\mathcal{C} : y^2 = x^3 + 486662x^2 + x$ sur \mathbb{F}_p , et le sous-groupe cyclique de \mathcal{C} engendré par le point P en $x = 9$
- Alice et Bob choisissent en secret des $a, b \in \mathbb{F}_p$ aléatoires (256 bits)
 - Puis calculent et s'échangent les points $A = aP, B = bP$
- Ils peuvent ensuite reconstruire le secret partagé $abP = aB = bA$

Plus petites clés et meilleures performances comparé à RSA

