

Établissement de clé

Algorithme de Diffie-Hellman sur les courbes elliptiques

G point générateur de la courbe

Hypothèse de sécurité: logarithme discret



Mon laptop

$$a \in \mathbb{Z}_n$$

$$\begin{array}{c} A = aG \\ \xrightarrow{\hspace{10em}} \\ \xleftarrow{\hspace{10em}} \\ B = bG \end{array}$$



inf8750.filenesless.dev

$$b \in \mathbb{Z}_n$$

Ex: Curve25519 from RFC 7748

$$\mathcal{C} = \{(x, y) \in \mathbb{F}_p : y^2 = x^3 + 486662x^2 + x\}$$

$$p = 2^{255} - 19, G \in \mathcal{C} \text{ point tel que } x = 9$$

$$\begin{aligned} s &= aB = abG \\ &= bA = abG \end{aligned}$$

