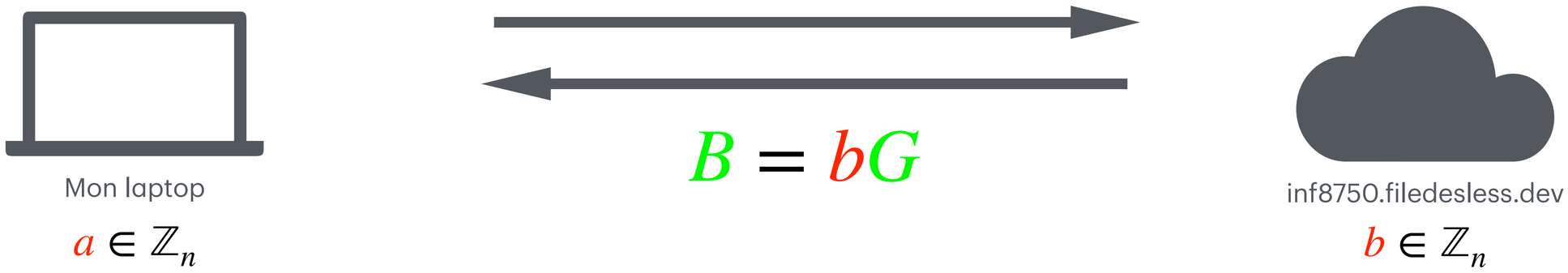
Établissement de clé

G point générateur de la courbe

Hypothèse de sécurité: logarithme discret

Algorithme de Diffie-Hellman sur les courbes elliptiques



Ex: Curve25519 from RFC 7748

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

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

$$s = aB = abG$$
$$= bA = abG$$