Établissement de clé

Utilisation des courbes elliptiques pour réduire la taille des clé

Symmetric Key Length	Standard asymmetric Key Length	Elliptic Curve Key Length
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

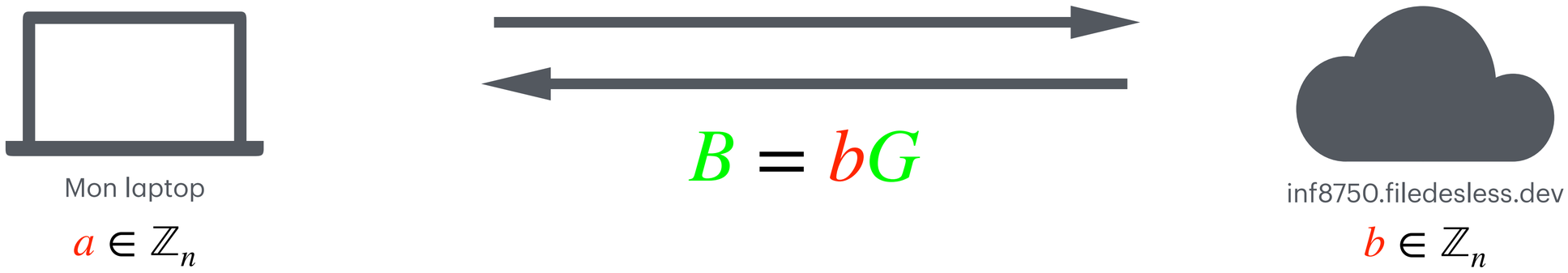
https://wiki.openssl.org/index.php/Elliptic_Curve_Cryptography

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 $x = 9$

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