Chiffrement asymétrique Diffie-Hellman

Christophe Viroulaud

Terminale NSI

Problématique

Le chiffrement symétrique est très efficace mais il souffre d'un défaut majeur : il faut que la source et le destinataire utilise la même clé de chiffrement.

Peut-on échanger une clé de manière sécurisée ?

Les mathématiques à la rescousse

- 1974 : Le puzzle de Merkle s'appuie sur le coût long du décryptage.

Les mathématiques à la rescousse

- 1974 : Le puzzle de Merkle s'appuie sur le coût long du décryptage.
- 1976 : **Diffie et Hellman** utilise une fonction mathématique avec des propriétés particulières

Propriétés

- La fonction f est connue de tous.

Propriétés

- La fonction f est connue de tous.
- Si on connaît $f(x, y)$ et x alors il est difficile de retrouver y.

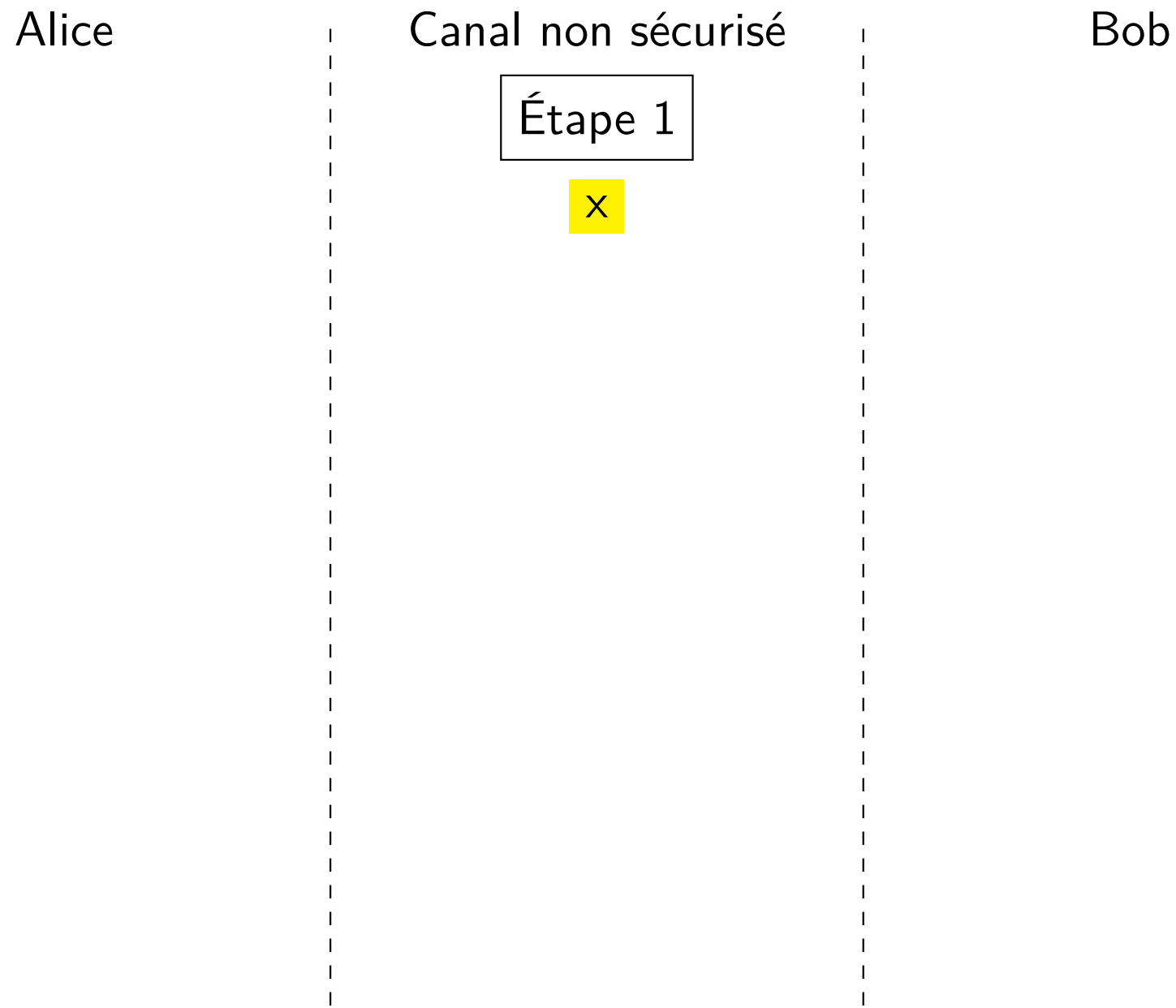
Propriétés

- La fonction f est connue de tous.
- Si on connaît $f(x, y)$ et x alors il est difficile de retrouver y.
- Pour tous entiers x, y, z,

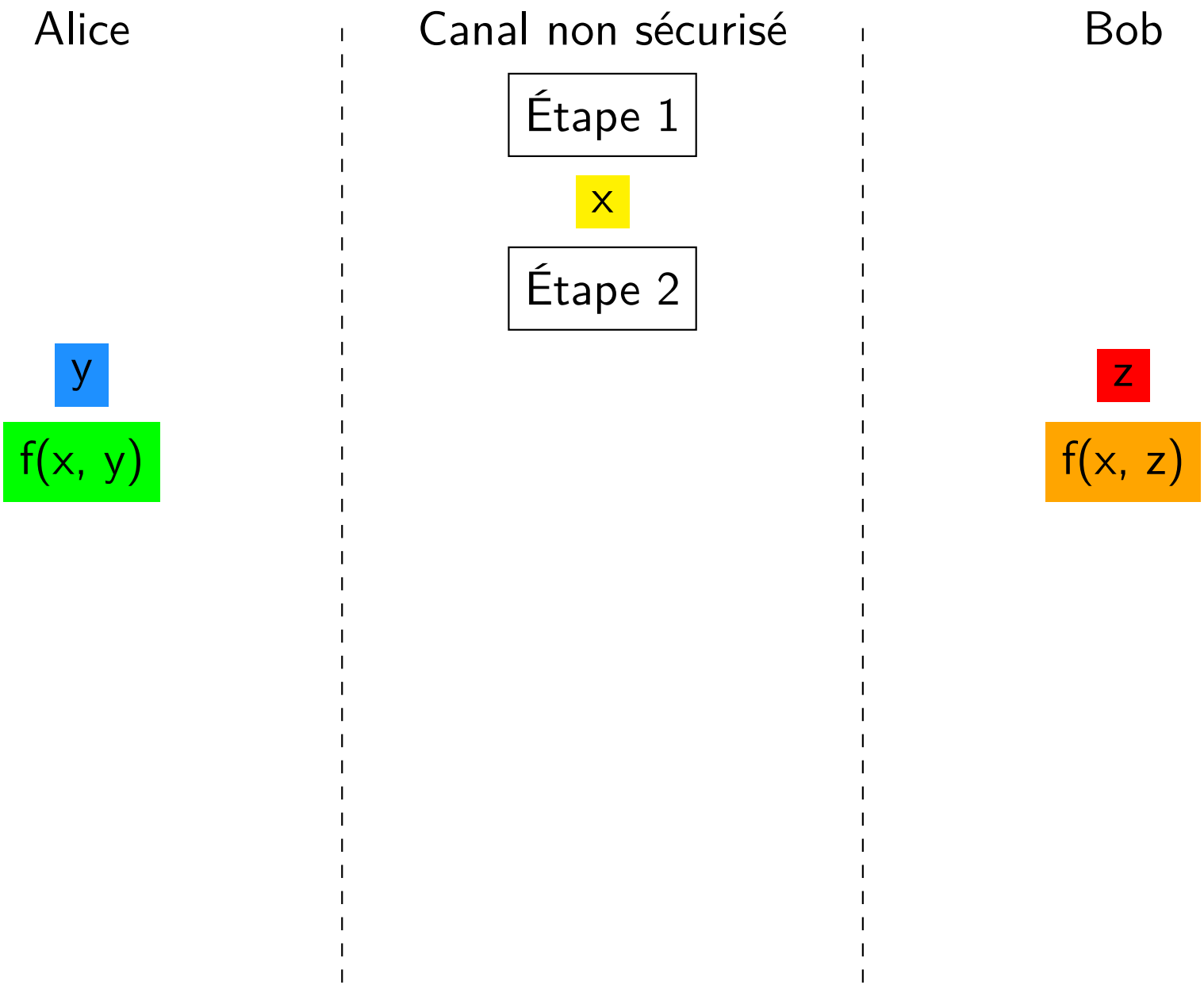
$$f(f(x, y), z) = f(f(x, z), y)$$

En pratique la fonction mathématique utilisée utilise les puissances et le modulo.

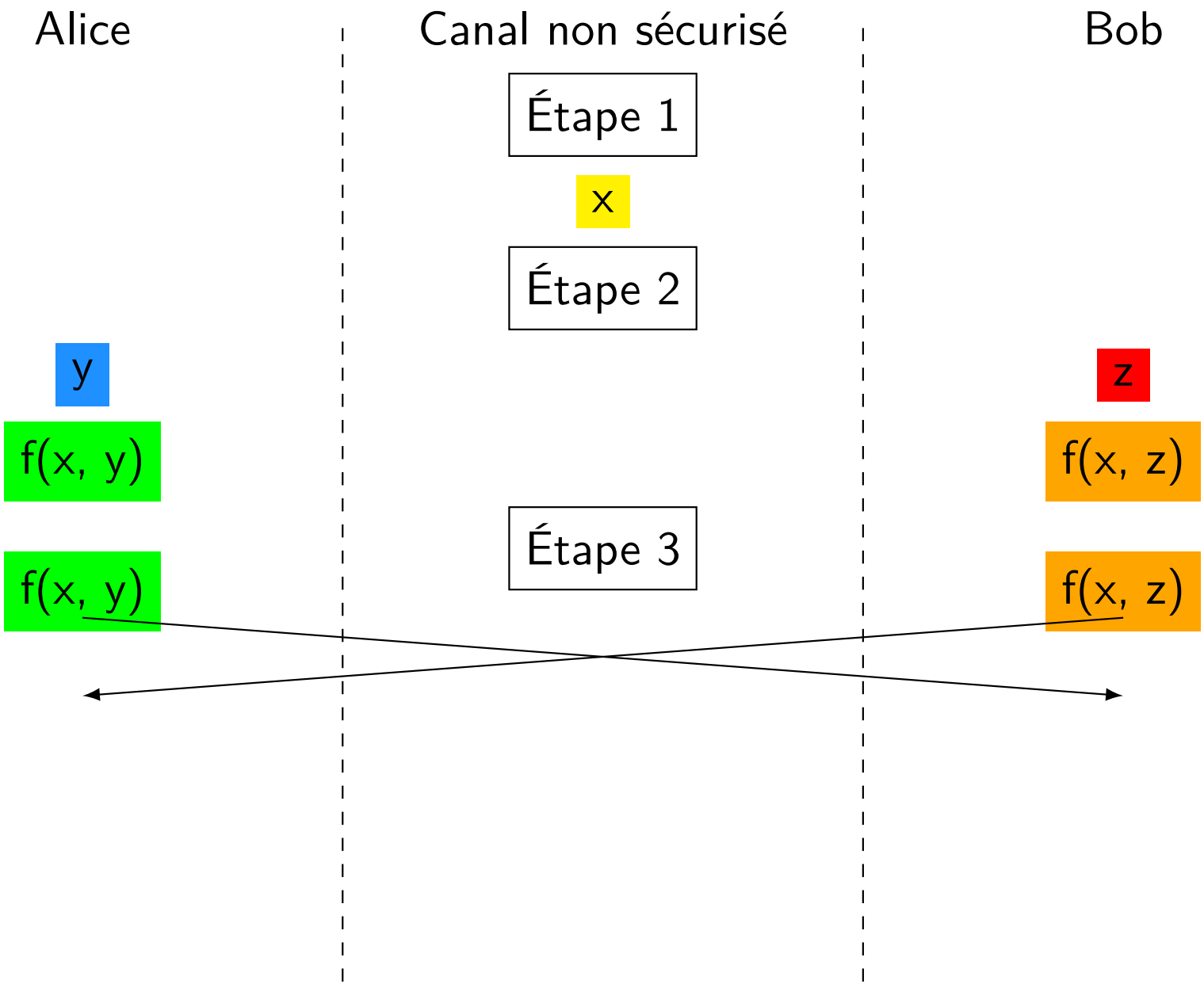
Analogie des couleurs



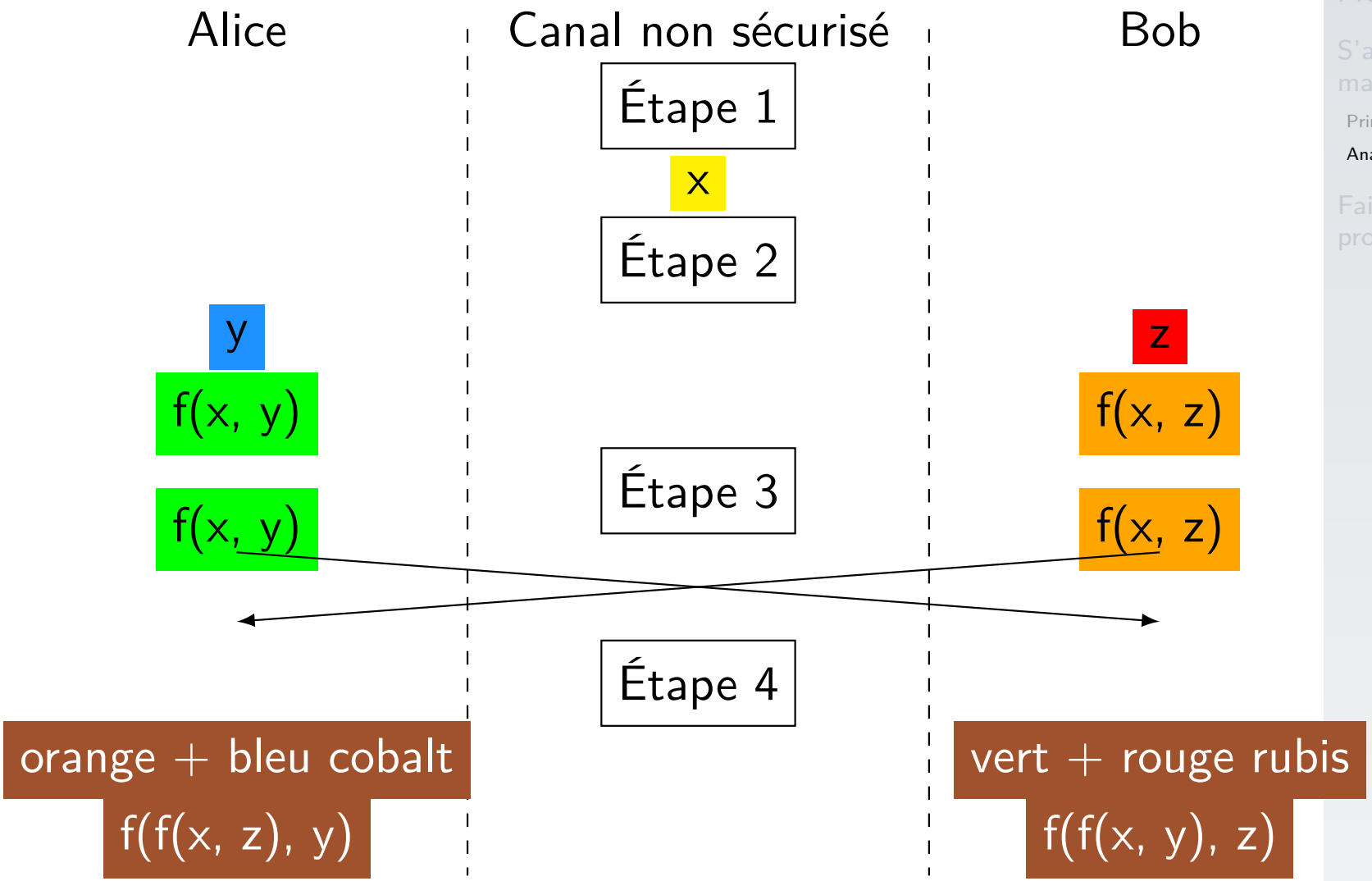
Analogie des couleurs



Analogie des couleurs



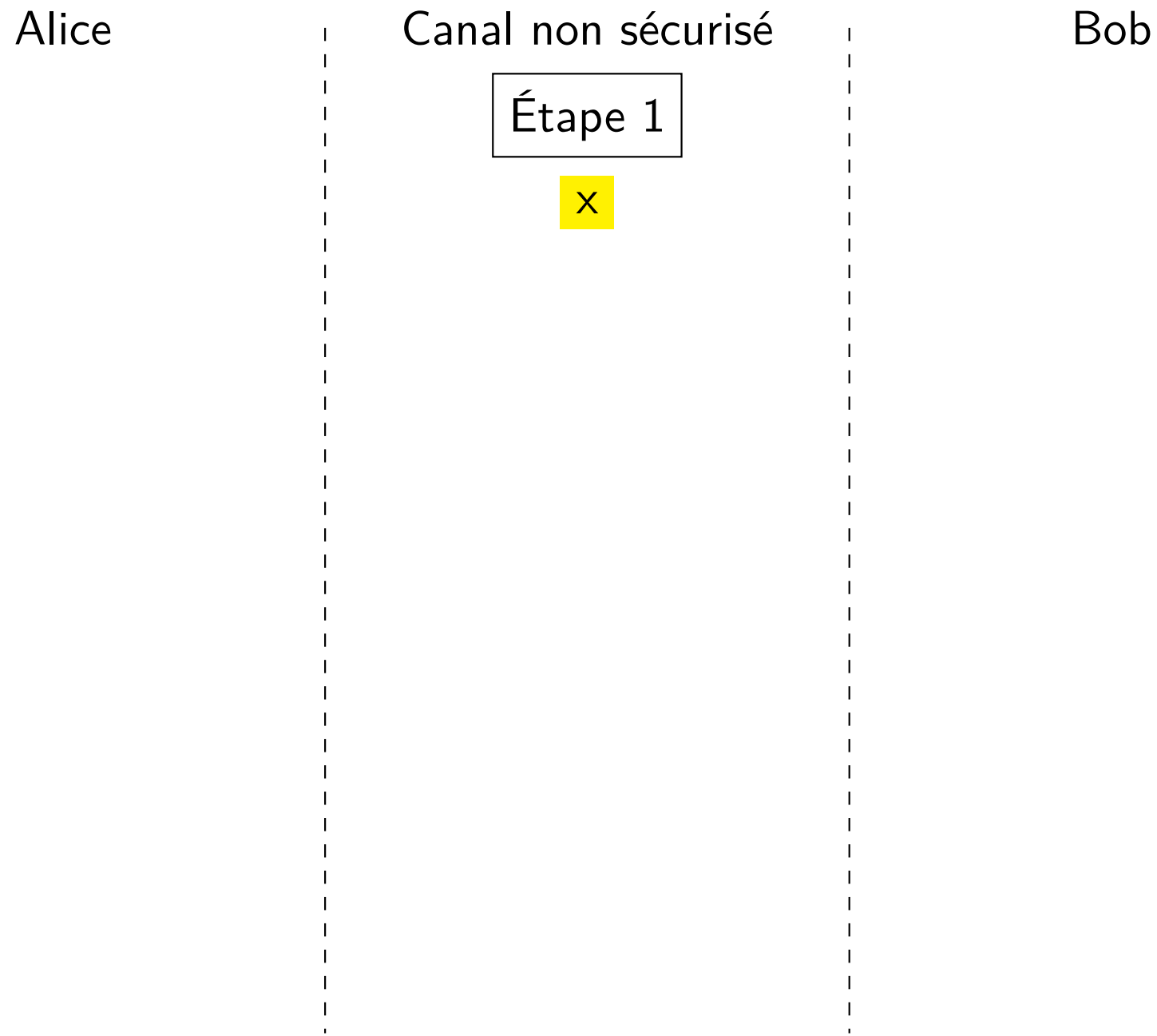
Analogie des couleurs



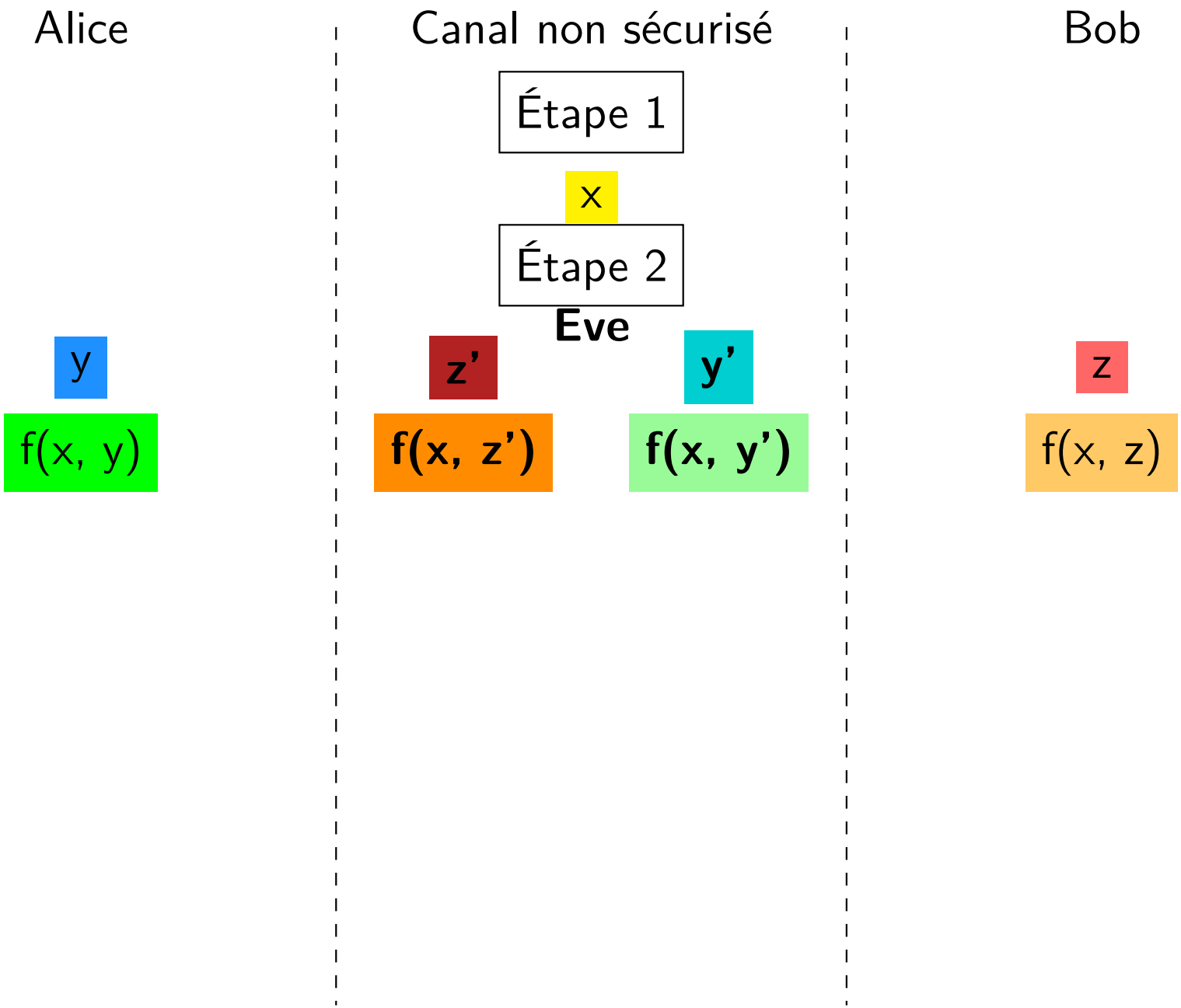
Faiblesse

Il est mathématiquement très difficile pour Eve (*eavesdropper : écouteuse*) de retrouver les valeurs choisies par Alice et Bob. Cependant, elle n'est pas obligée de le faire.

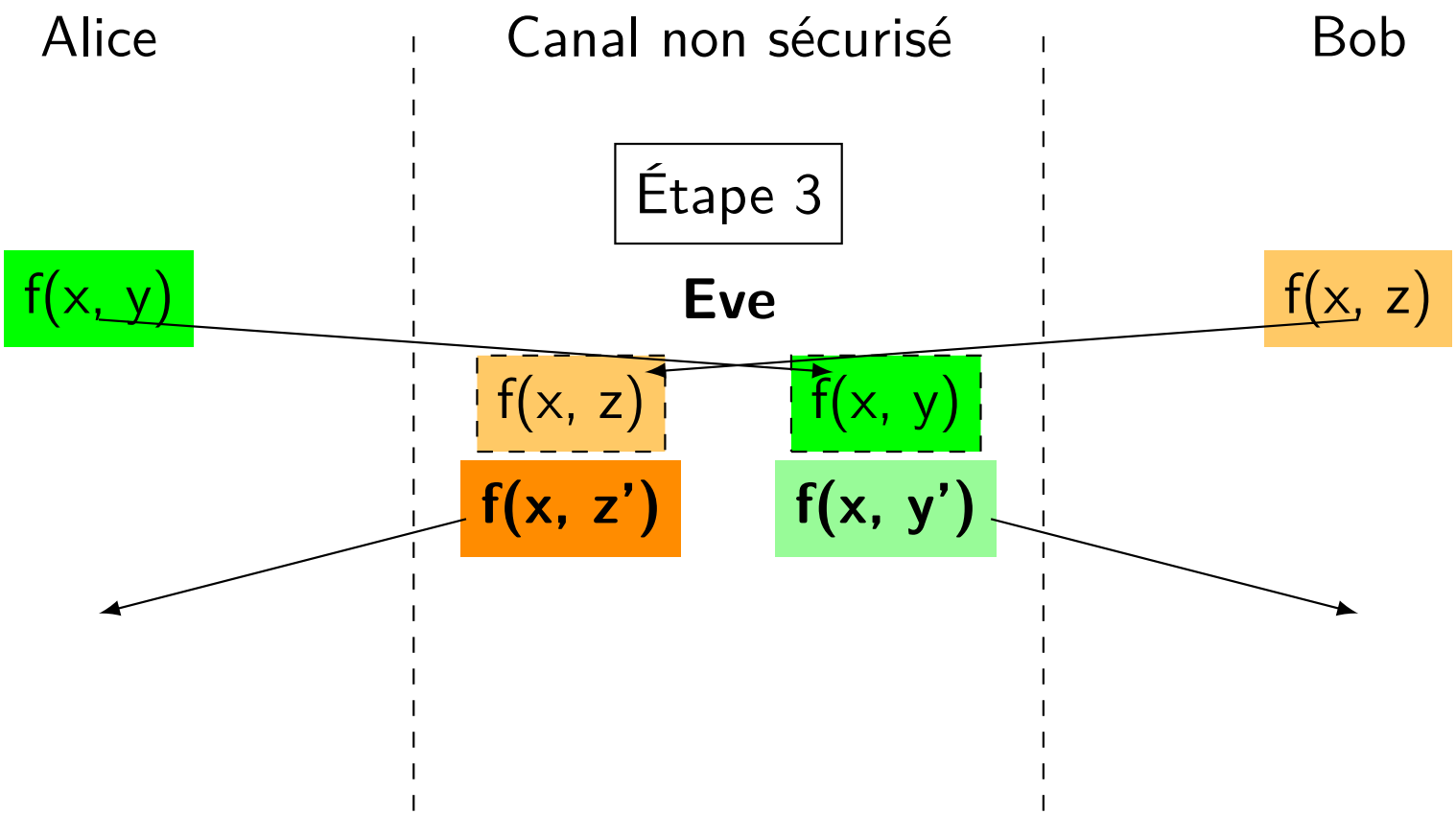
Man in the middle attack



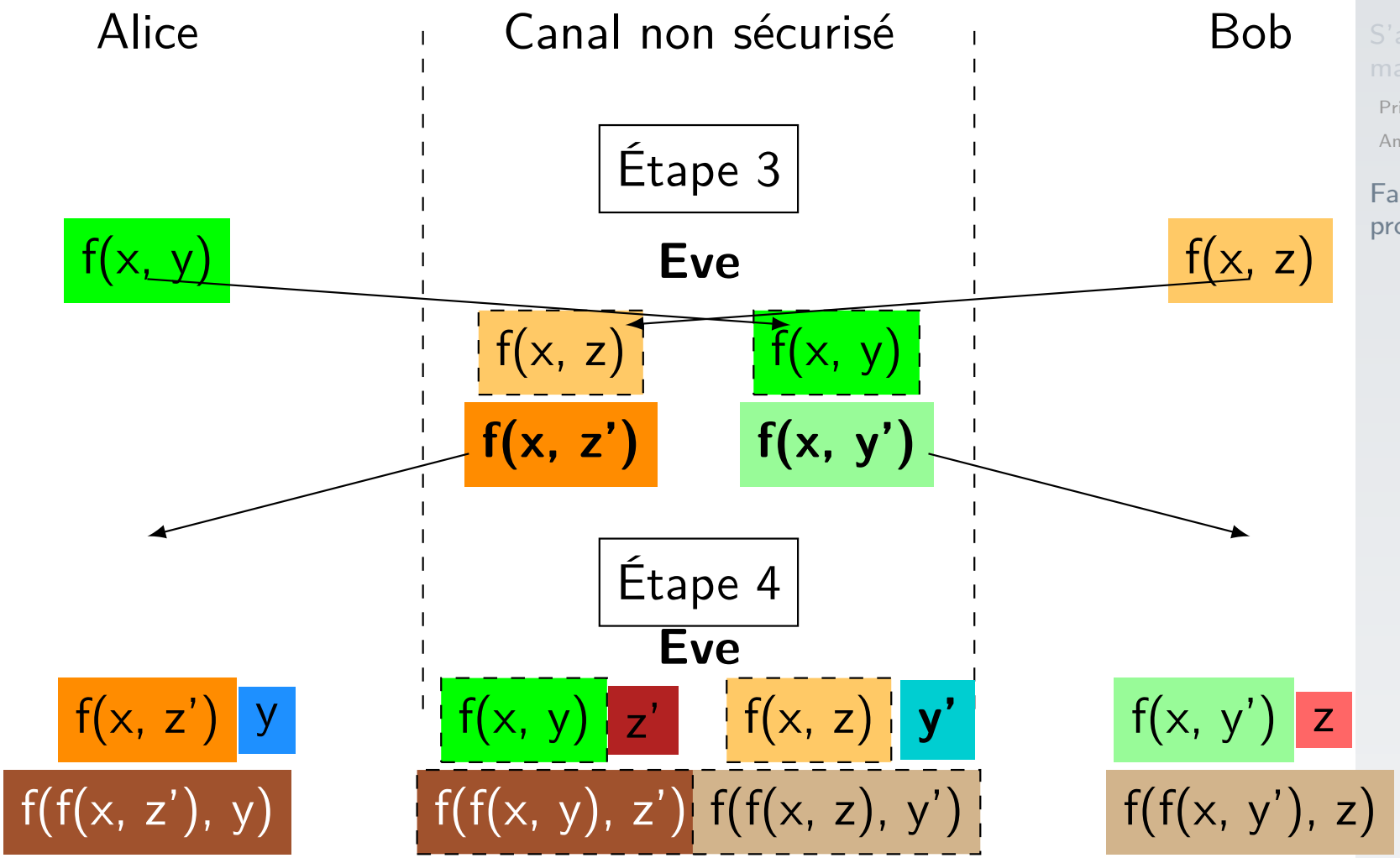
Man in the middle attack



Man in the middle attack



Man in the middle attack



À retenir

Le protocole de Diffie-Hellman permet d'échanger des clés par un canal non sécurisé. Cependant il n'assure pas l'*authentification* des participants.