Chiffrement asymétrique de Diffie-Hellman

Christophe Viroulaud

Terminale - NSI

Archi 22

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 ?

Sommaire

S'aider des mathématiques

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

S'aider des mathématiques

- 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.

FIGURE 1 – Prix Turing 2015 : Whitfield Diffie et Martin Hellman

- La fonction f est connue de tous.

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

- 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,

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

À retenir

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

Sommaire

Analogie des couleurs

Observation

Classiquement la méthode de Diffie-Hellman est présentée par une analogie de mélanges de couleurs.

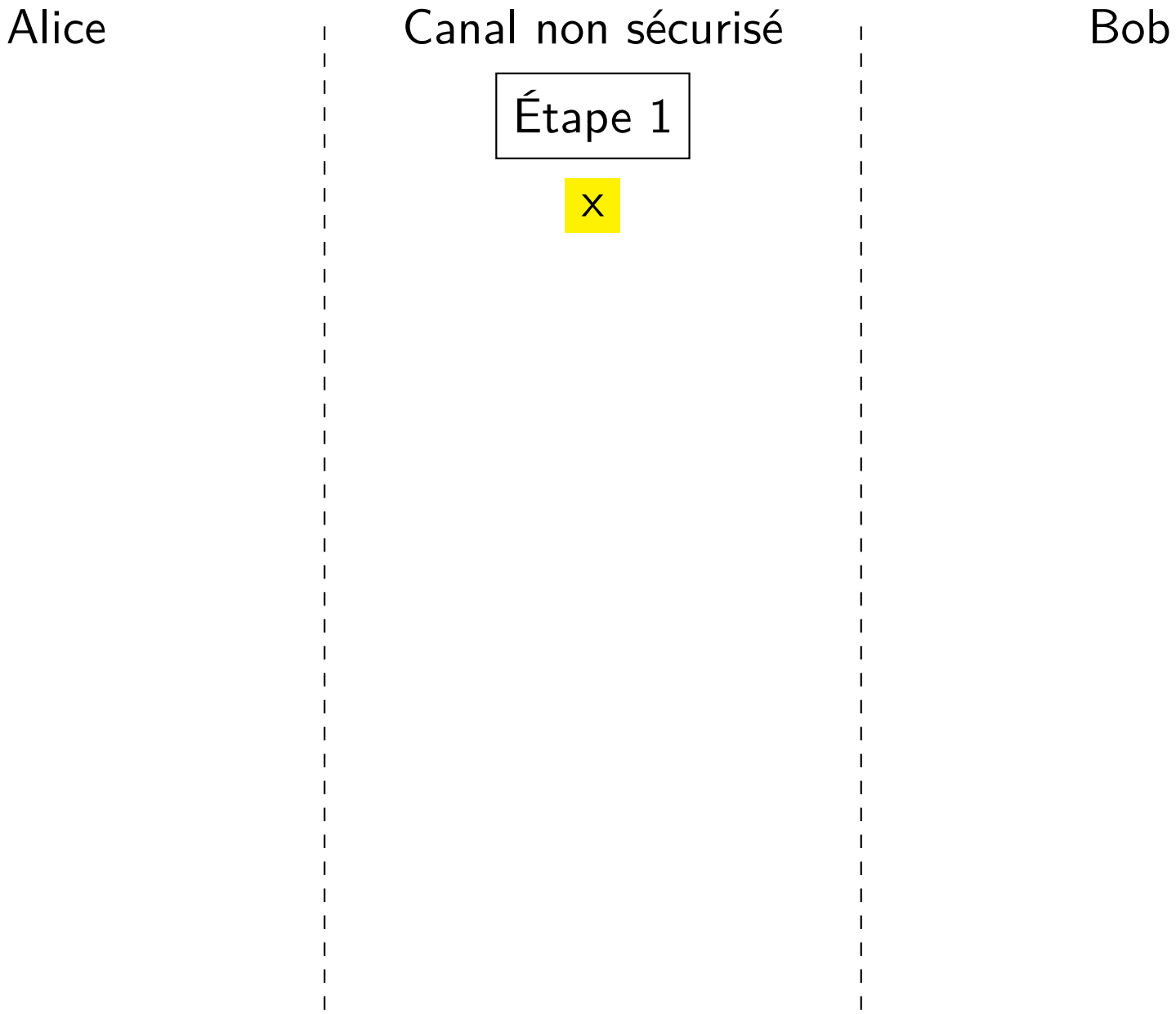


FIGURE 2 – **clé publique :** une couleur commune est choisie.

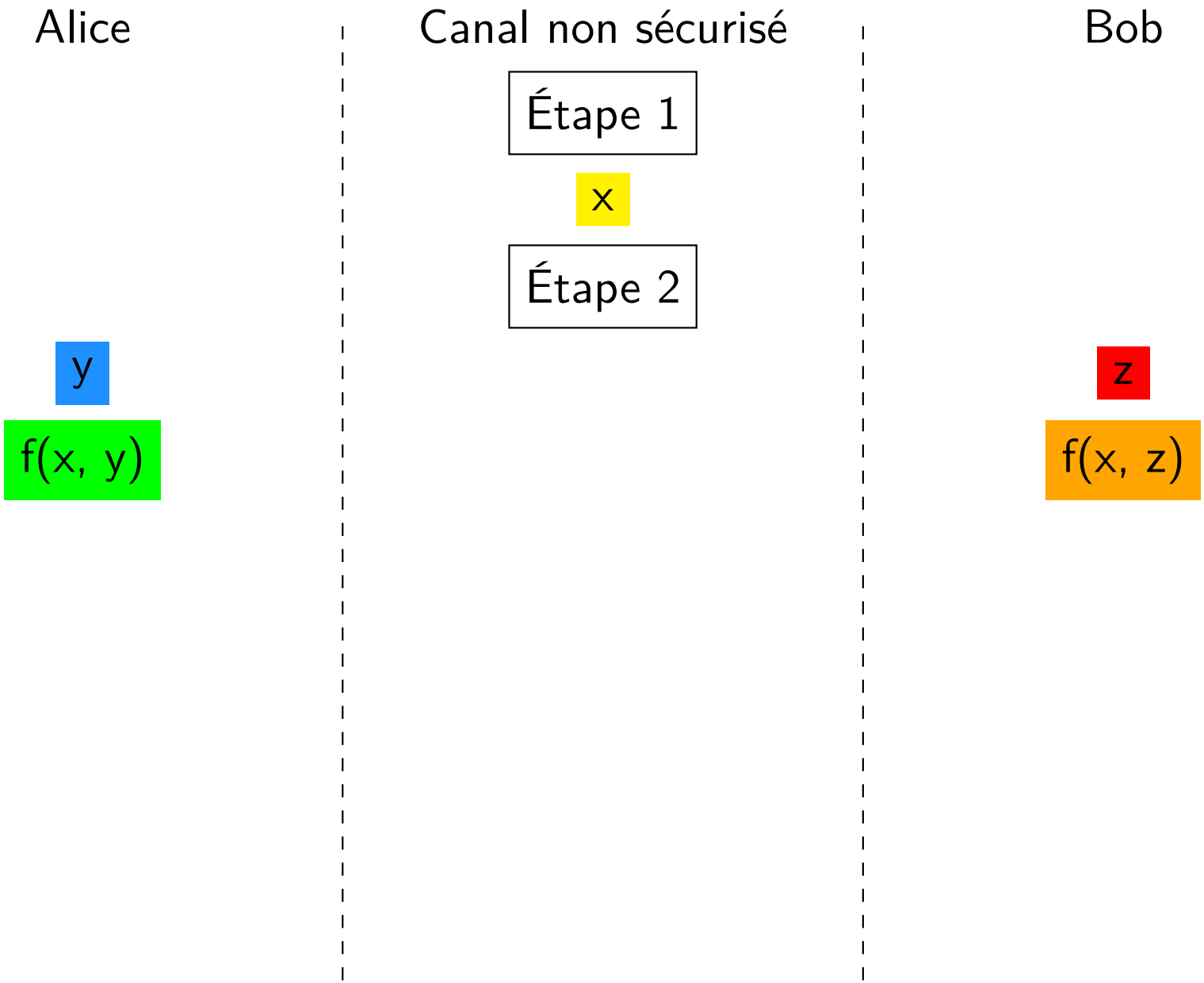


FIGURE 3 – **Clé privée :** chaque individu choisie une couleur et la *mélange* avec la couleur commune.

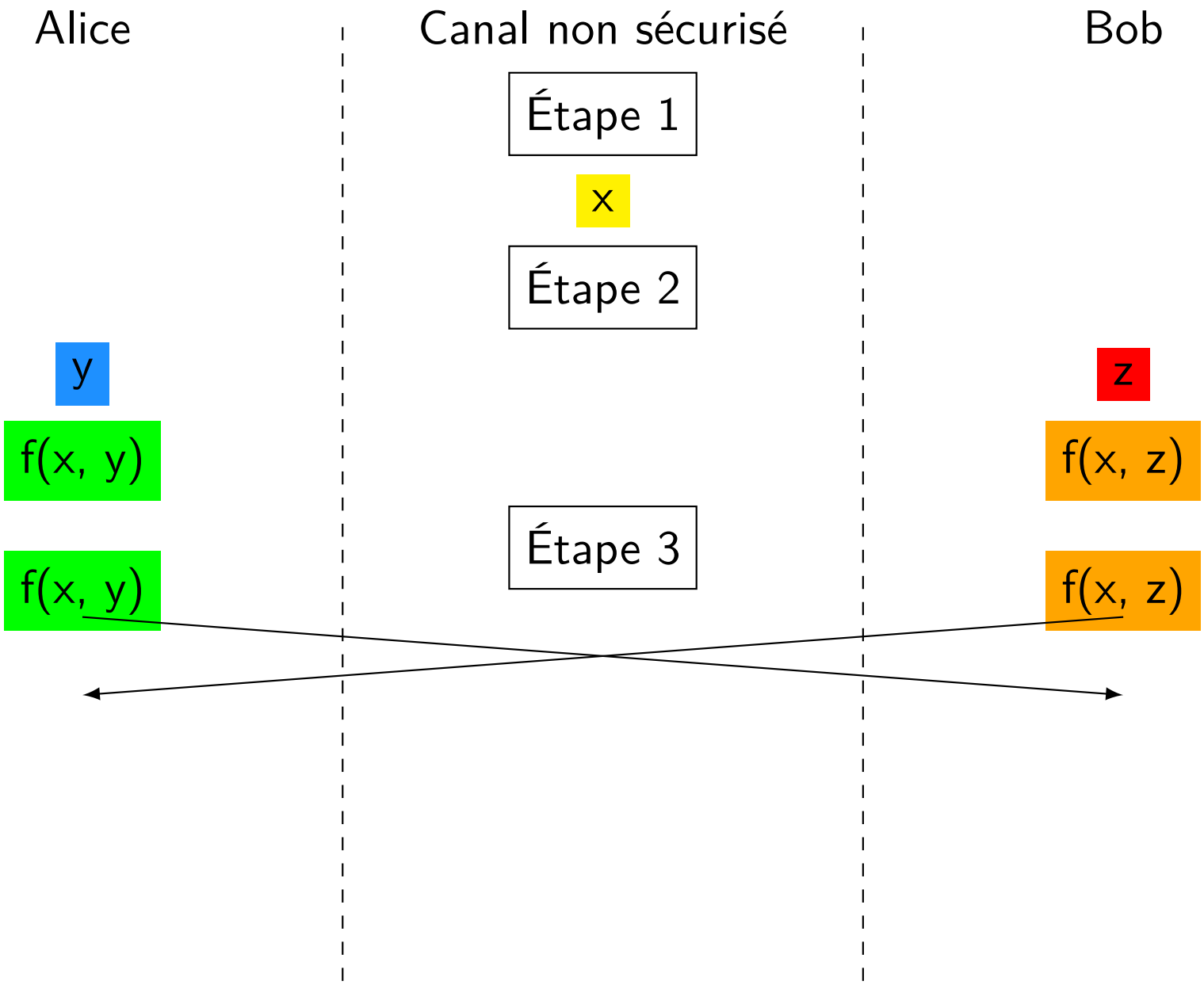


FIGURE 4 – Chaque individu partage sa couleur.

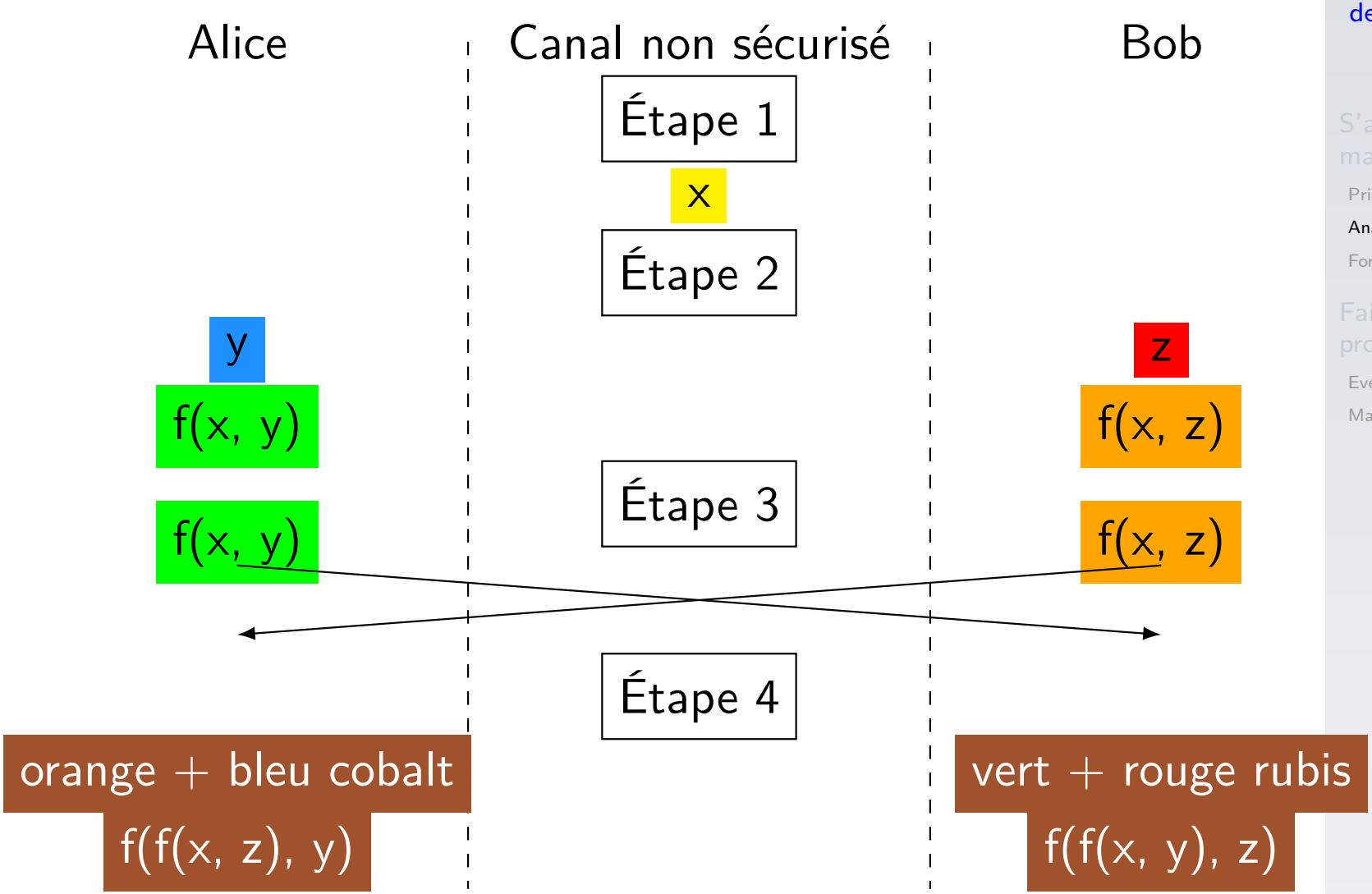


FIGURE 5 – Chaque individu mélange la couleur reçue avec la couleur privée.

Observation

Alice et Bob utilisent le (même) marron comme clé de chiffrement.

Sommaire

Formalisme mathématique

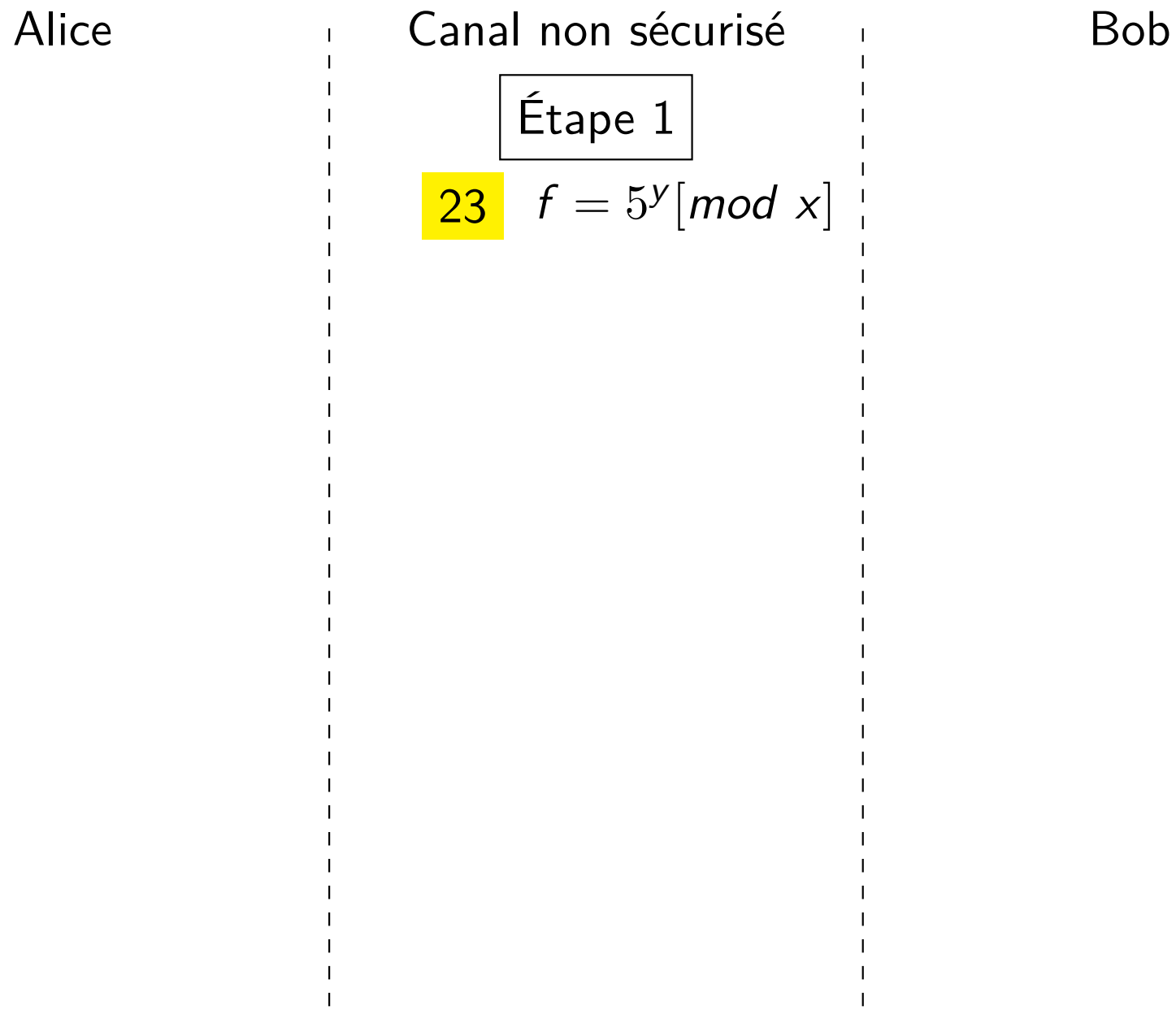


FIGURE 6 – **clé publique :** une couleur commune est choisie.

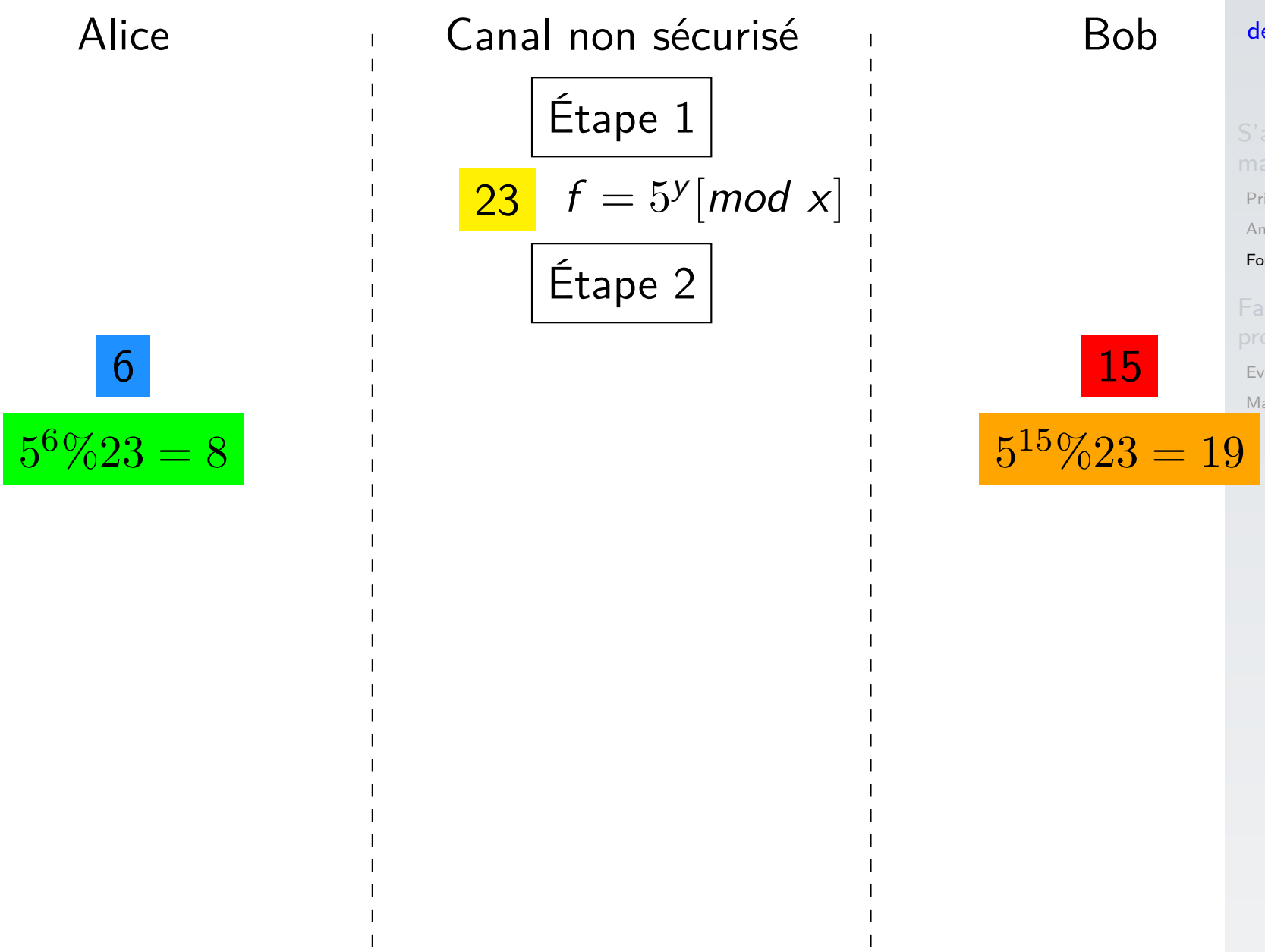


FIGURE 7 – **Clé privée :** chaque individu choisie une couleur et la *mélange* avec la couleur commune.

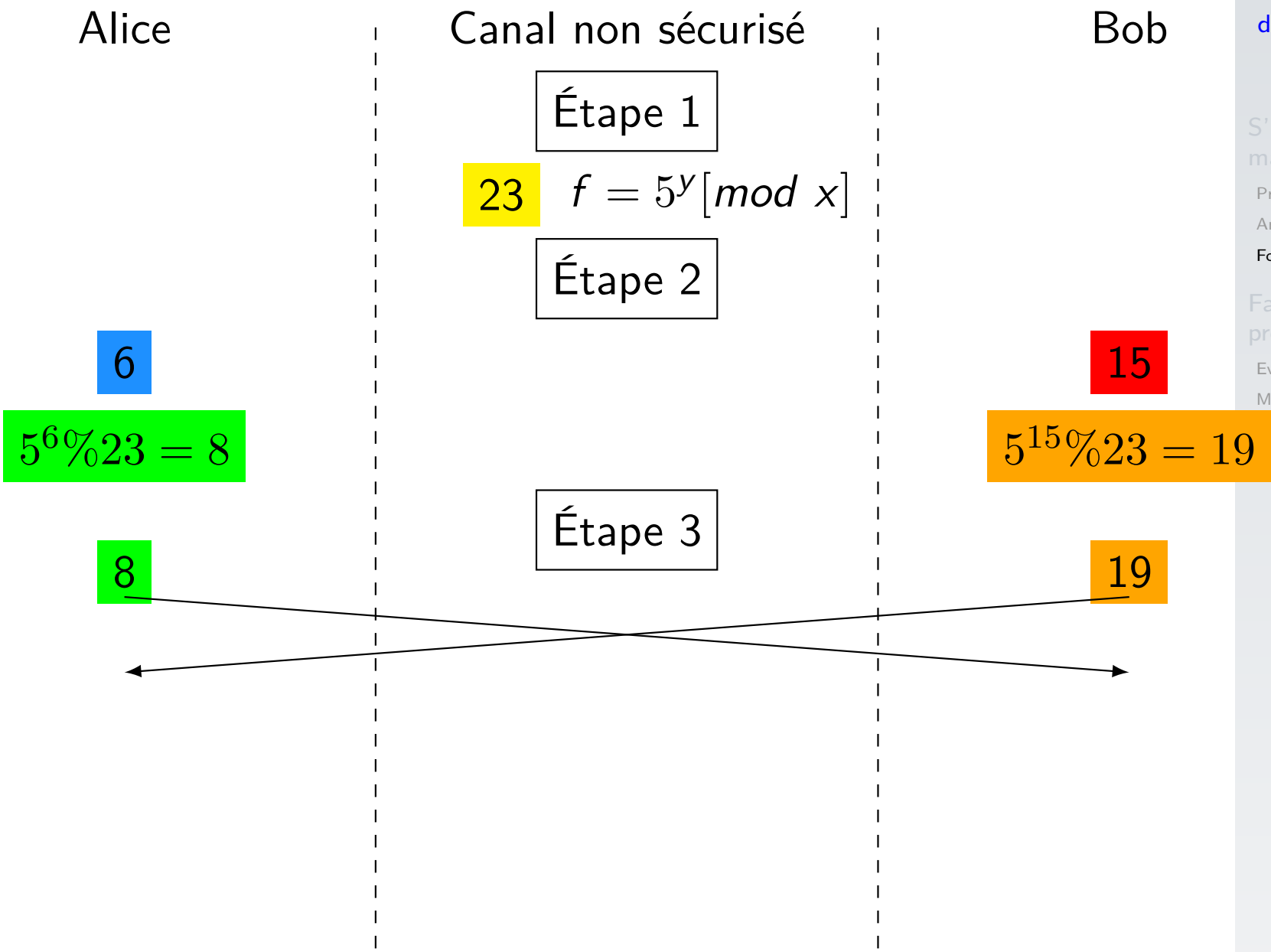


FIGURE 8 – Chaque individu partage sa couleur.

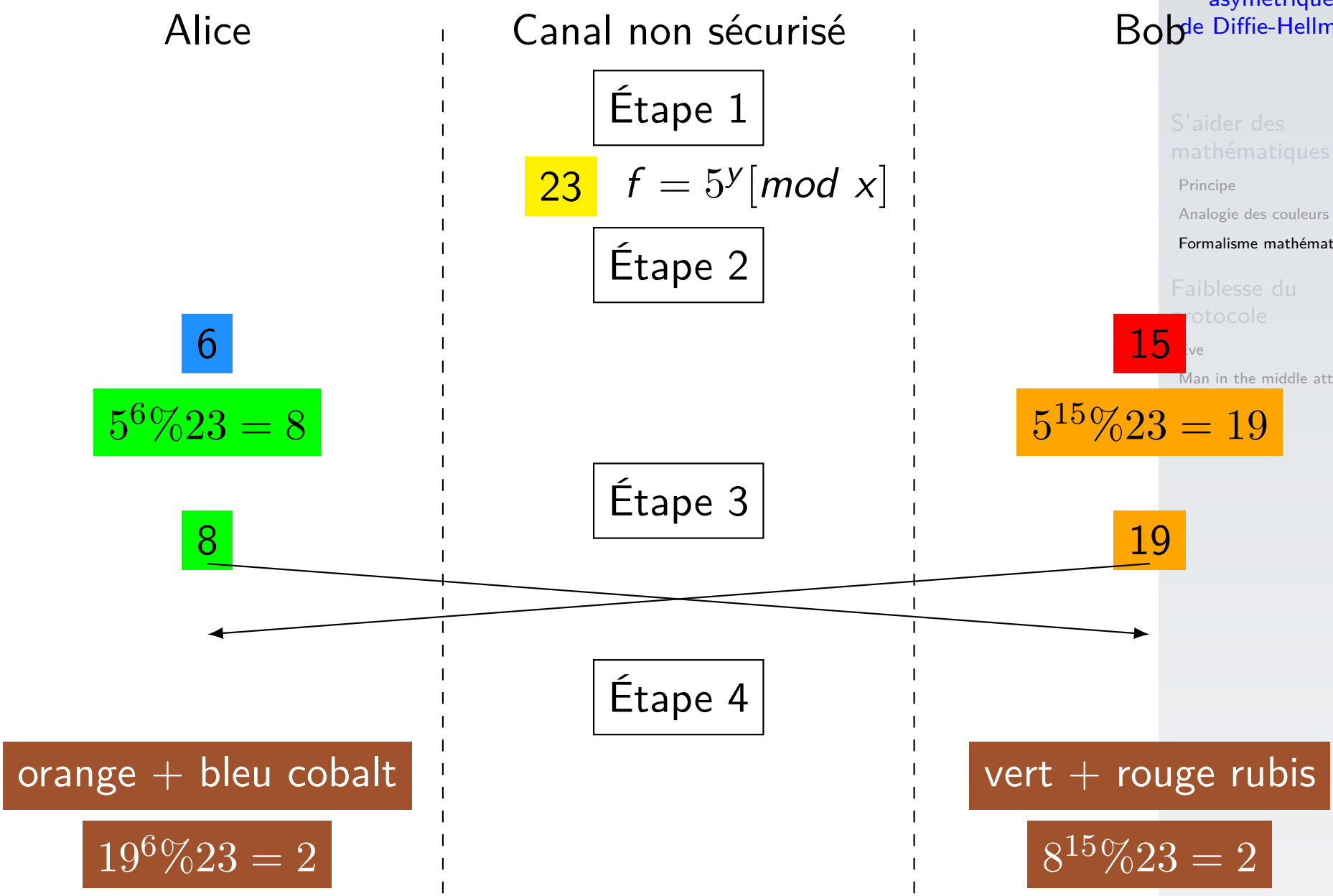


FIGURE 9 – Chaque individu mélange la couleur reçue avec la couleur privée.

À retenir

En pratique on utilise des nombres très grands afin qu'une attaque par force brute ne soit pas efficace.

Sommaire

Faiblesse du protocole - Eve

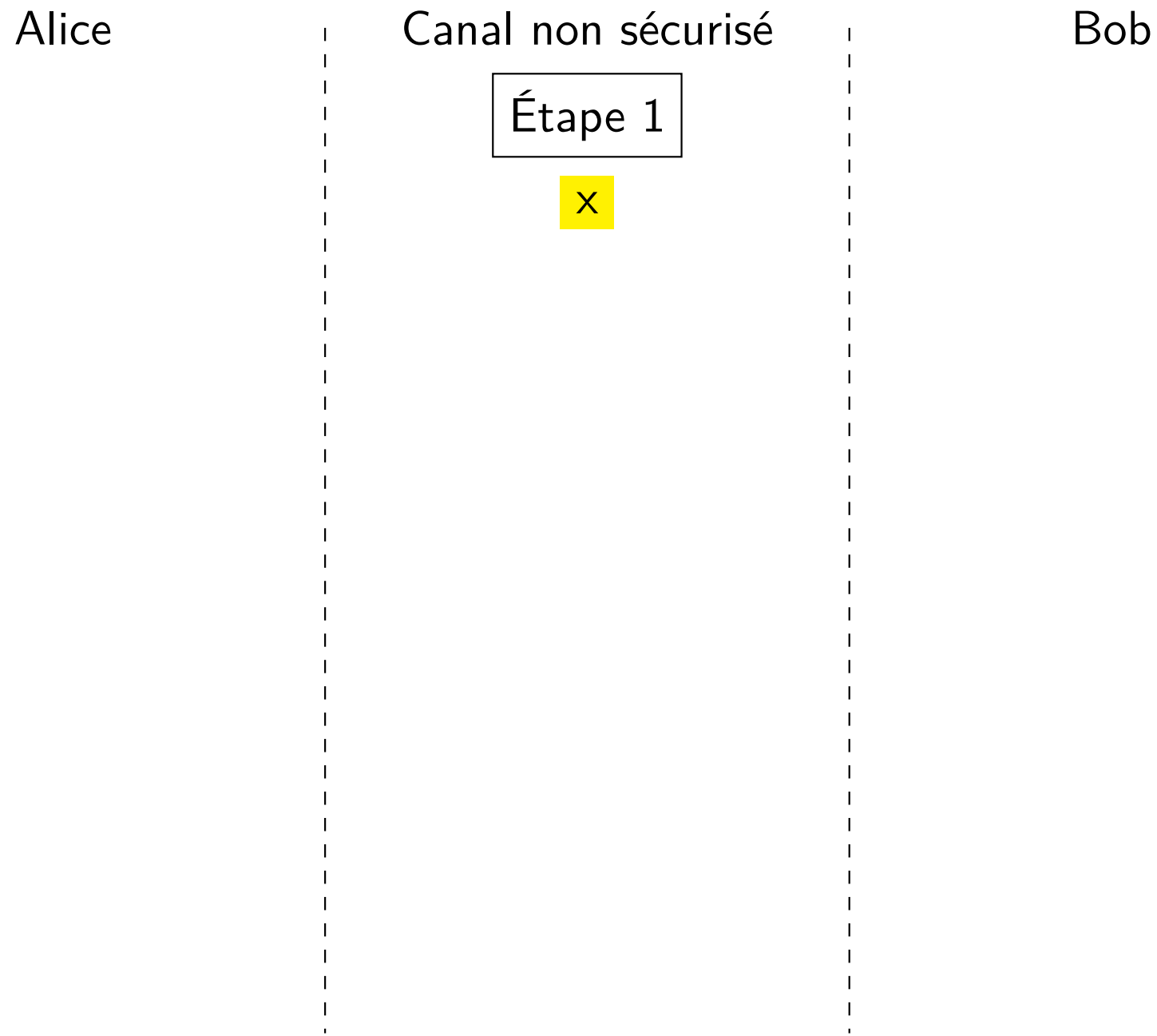
Dans la démonstration, Eve est un personnage qui tente de décrypter le message.

À retenir

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.

Sommaire

Man in the middle attack



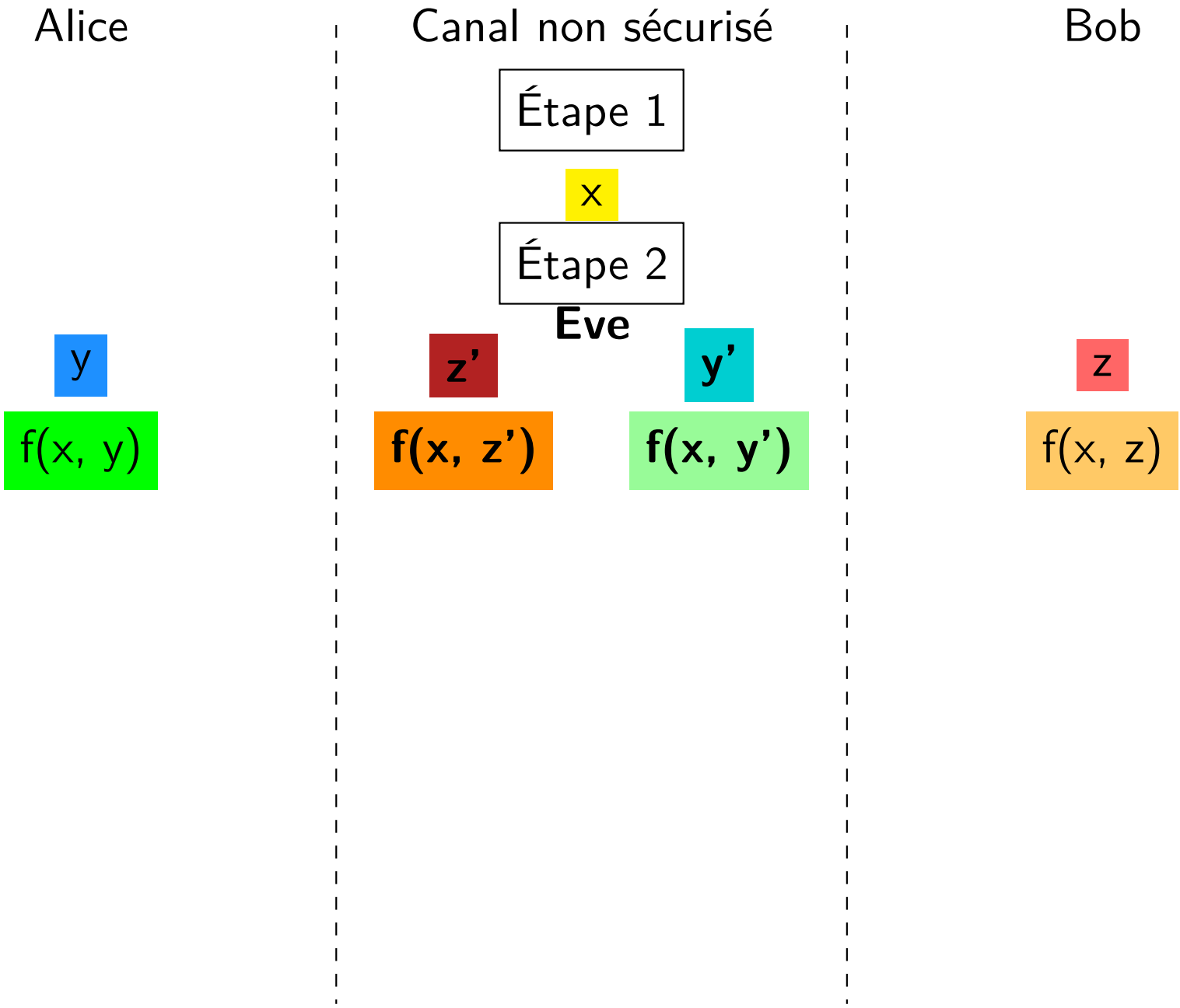


FIGURE 10 – Eve se fait passer pour le destinataire de chaque individu.

Man in the middle attack

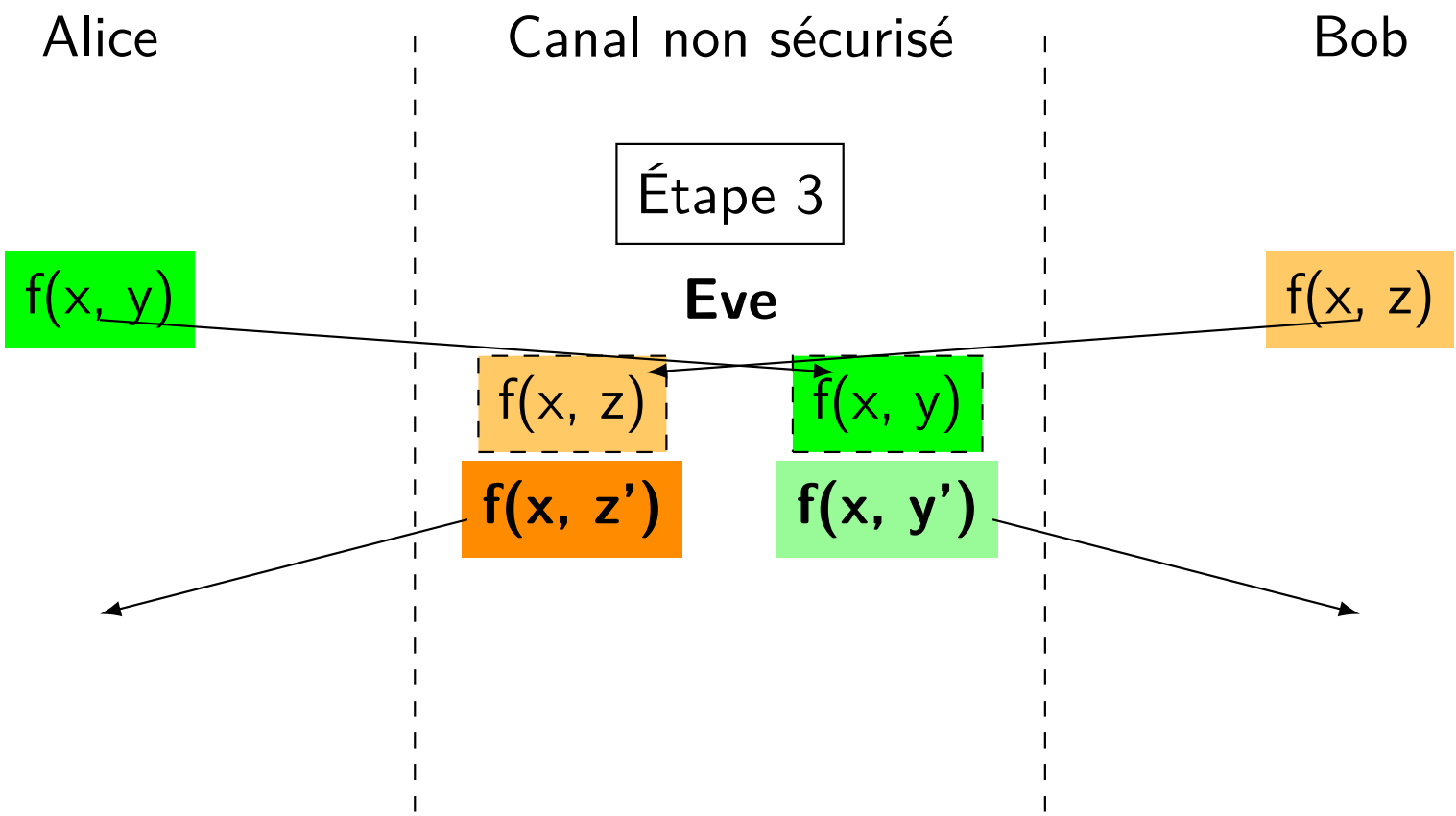


FIGURE 11 – Il n'est pas possible pour Alice et Bob d'être sûr de communiquer avec la bonne personne.

Man in the middle attack

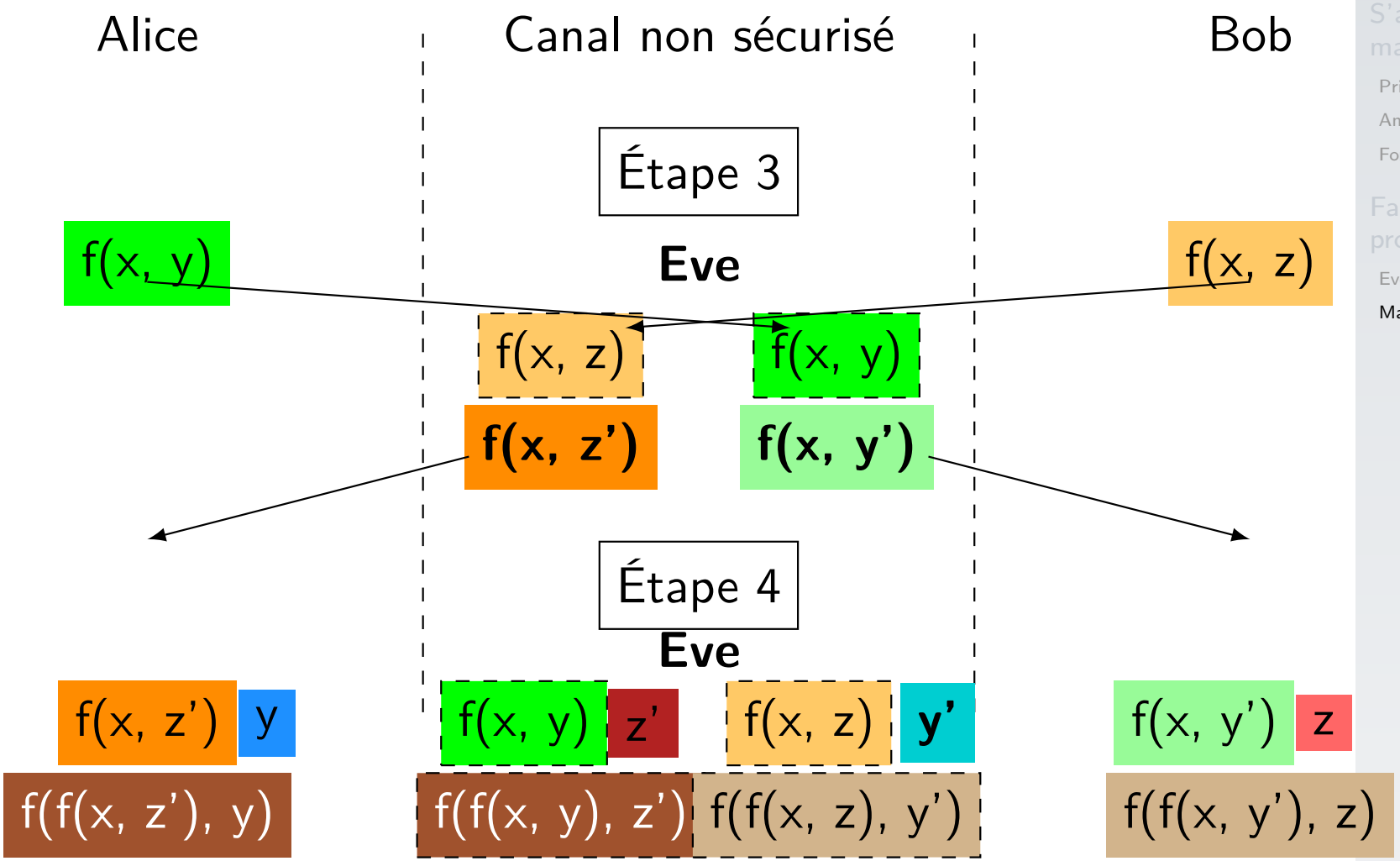


FIGURE 12 – Eve produit des clés pour chaque destinataire.

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.