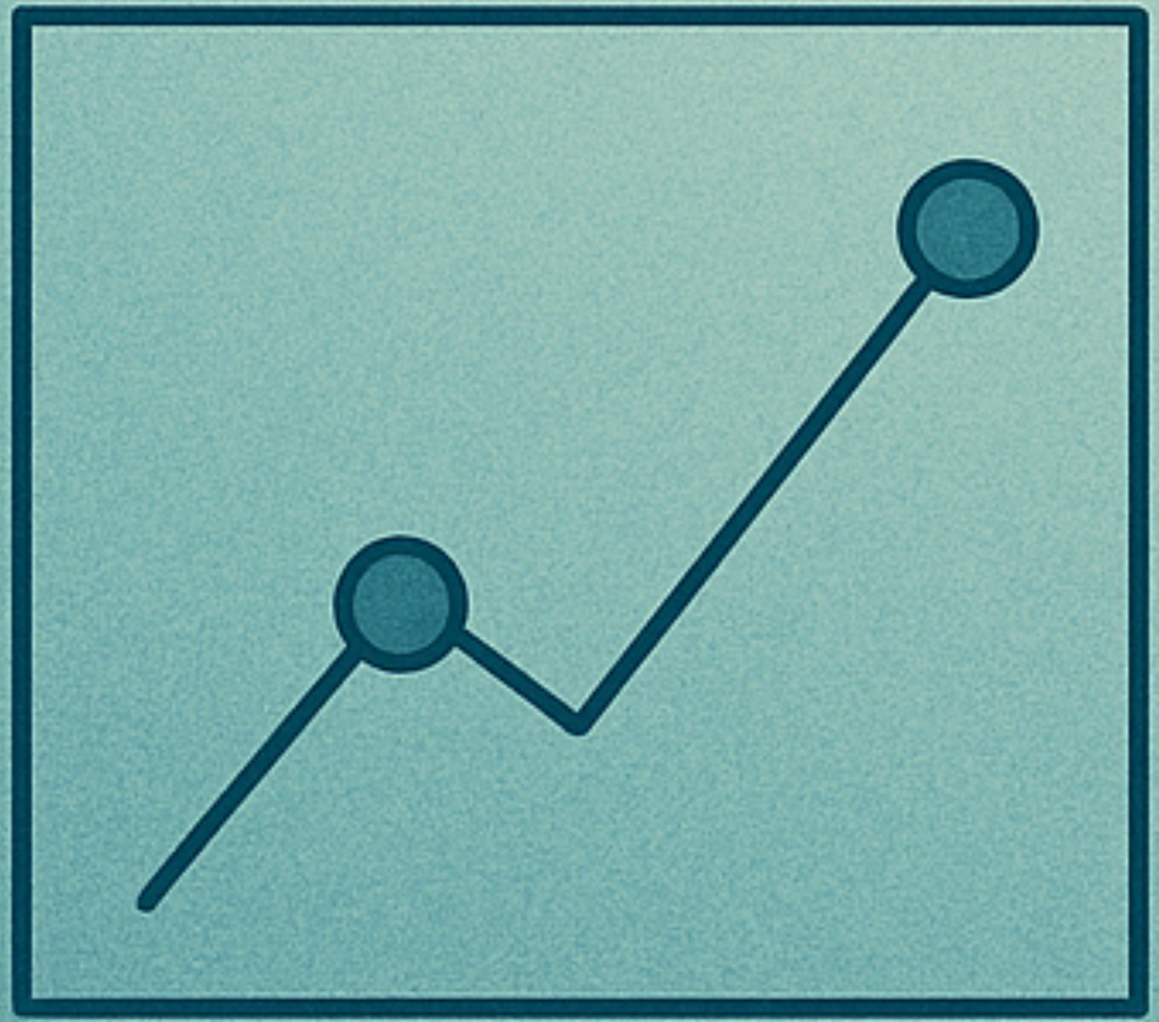
IRIF
INSTITUT
DE RECHERCHE
EN INFORMATIQUE
FONDAMENTALE

Université
Paris Cité

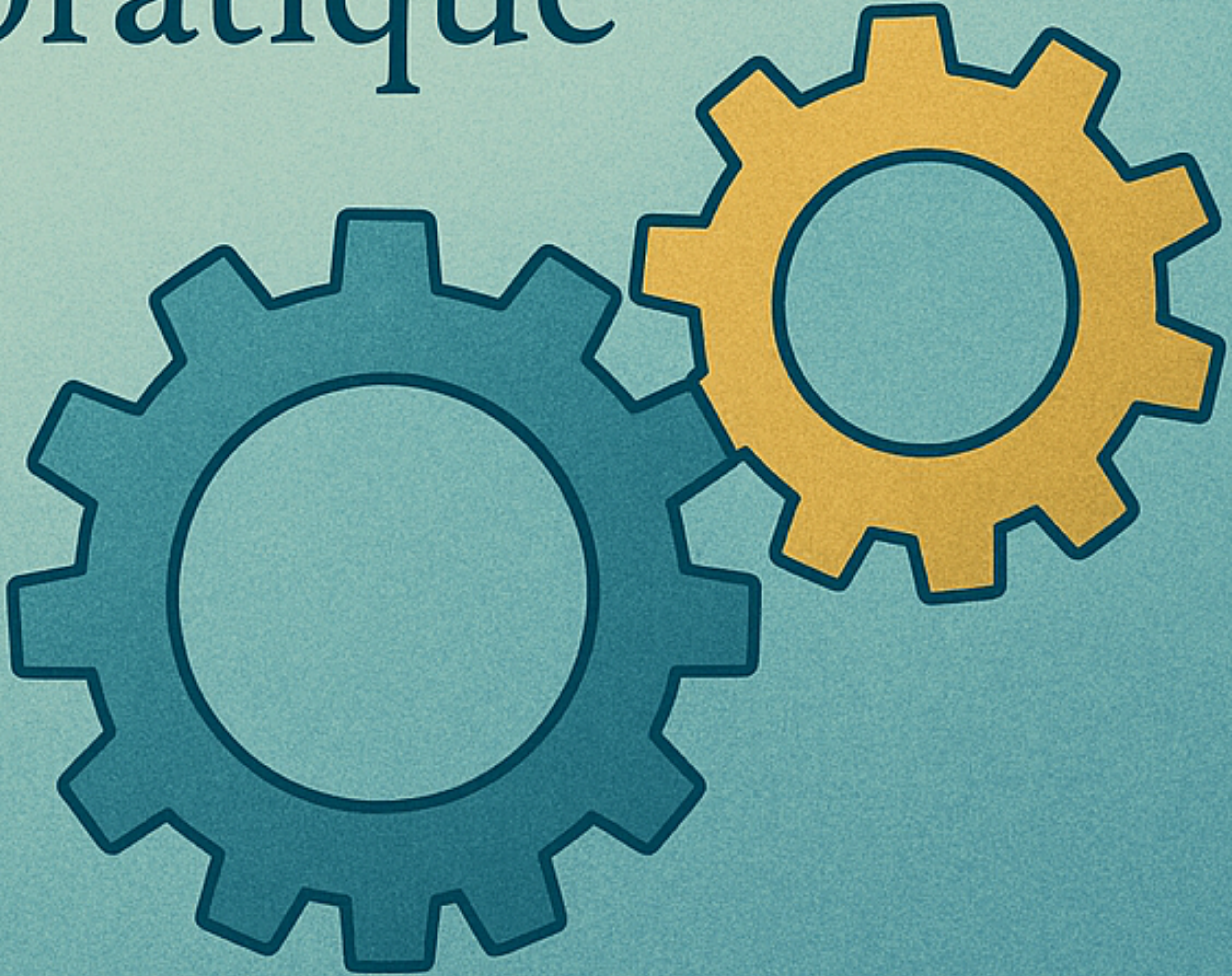
cnrs

Calcul sécurisé et aléa corrélé :

de la théorie à la pratique



Geoffroy Couteau



Calcul sécurisé et aléa corrélé

Dans ce cours, nous verrons :

- Quelques rappels sur le calcul sécurisé et les transferts inconscients
- Pourquoi l'approche originelle de Goldreich, Micali, et Wigderson est inefficace
- Comment faire passer le calcul sécurisé à l'échelle *efficacement*

Objectifs :

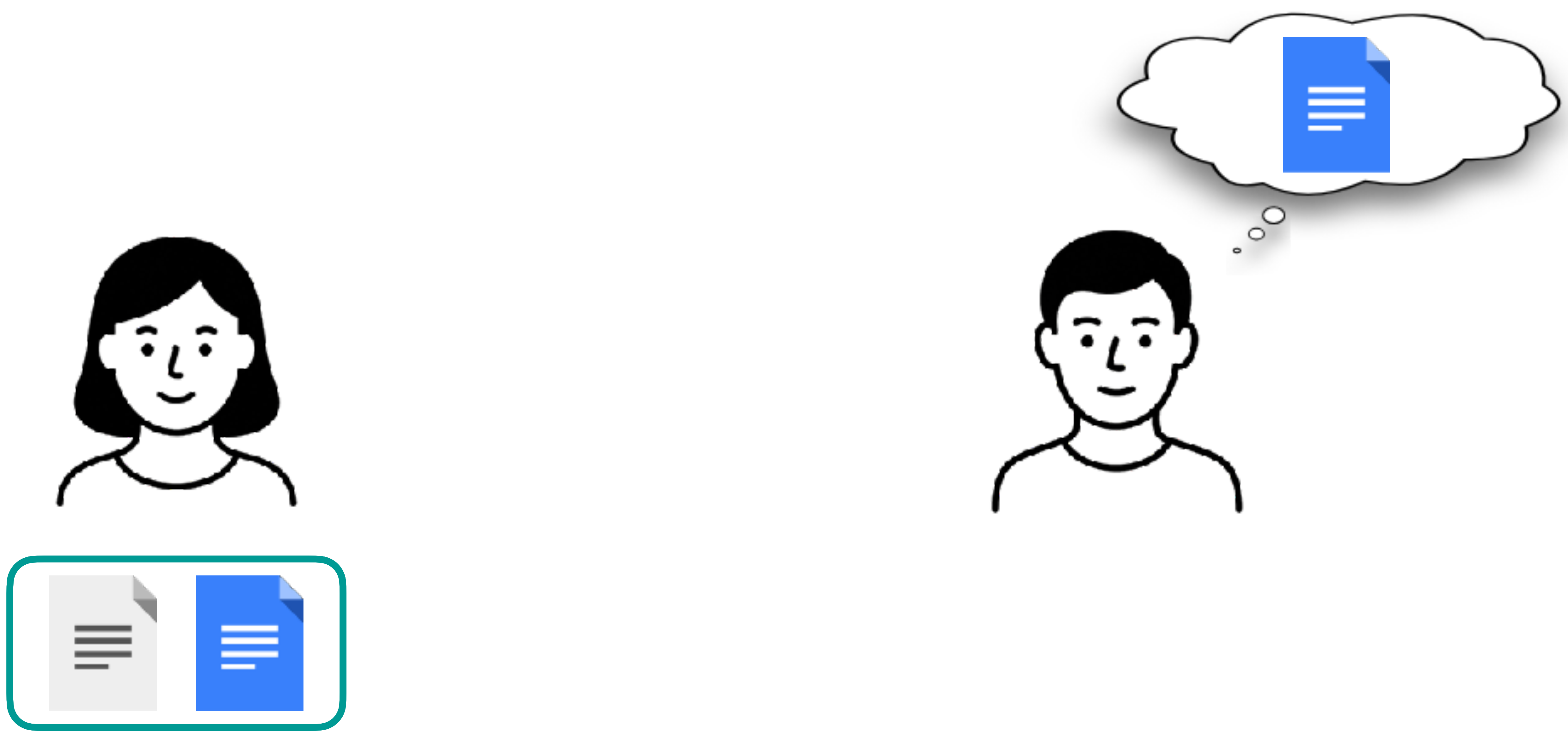
- Vous donner une intuition du coût de la cryptographie : quand on conçoit un nouveau protocole, *concrètement*, combien de temps ça prend de le faire tourner ?
- Au travers d'interludes et d'analogies, vous donner une intuition des choix stratégiques qui sont réalisés et des approches qui sont choisies.

Certains aspects abordés vers la fin du cours seront plus techniques. Cependant, l'intuition des coûts, le message général, et les outils introduits durant les interludes, peuvent tous être compris aisément même sans suivre les parties plus techniques.

Xxx/s

Transfert Inconscient

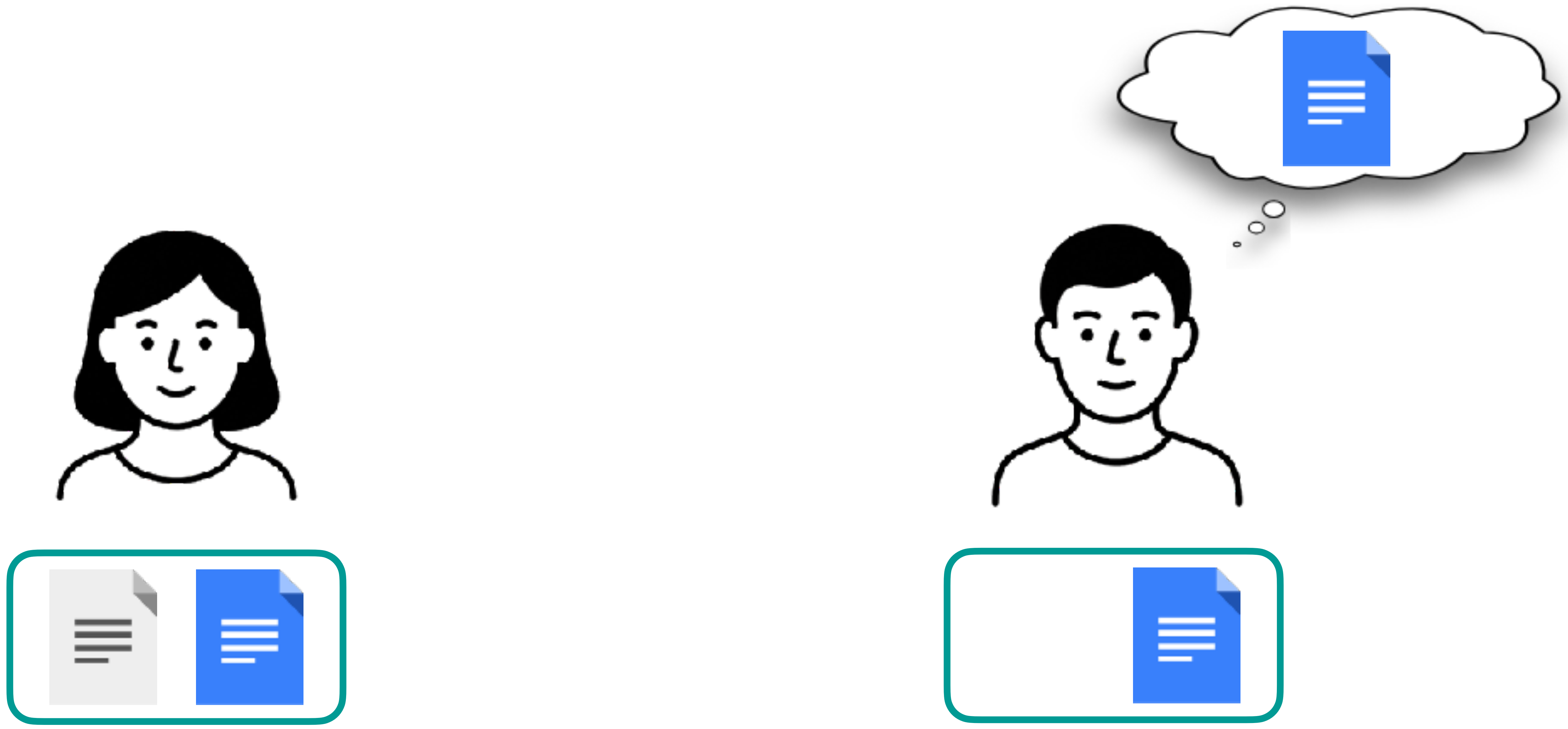
RAPPEL DE COURS



- Alice possède deux documents, Bob veut apprendre l’un d’entre eux
- Alice souhaite révéler au plus un document
- Bob ne veut pas révéler son choix

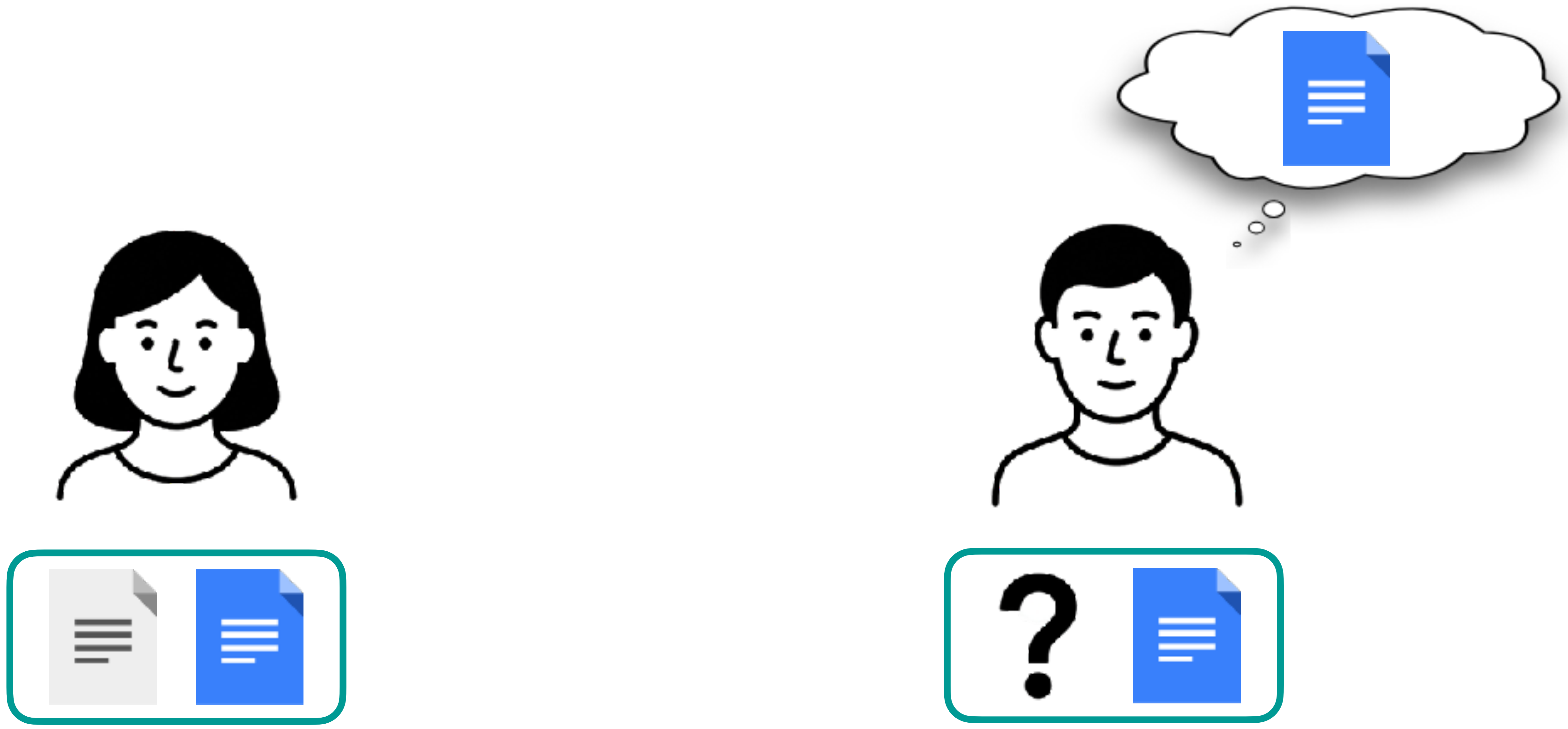
Transfert Inconscient

RAPPEL DE COURS



►
- Alice possède deux documents, Bob veut apprendre l’un d’entre eux
- Alice souhaite révéler au plus un document
- Bob ne veut pas révéler son choix

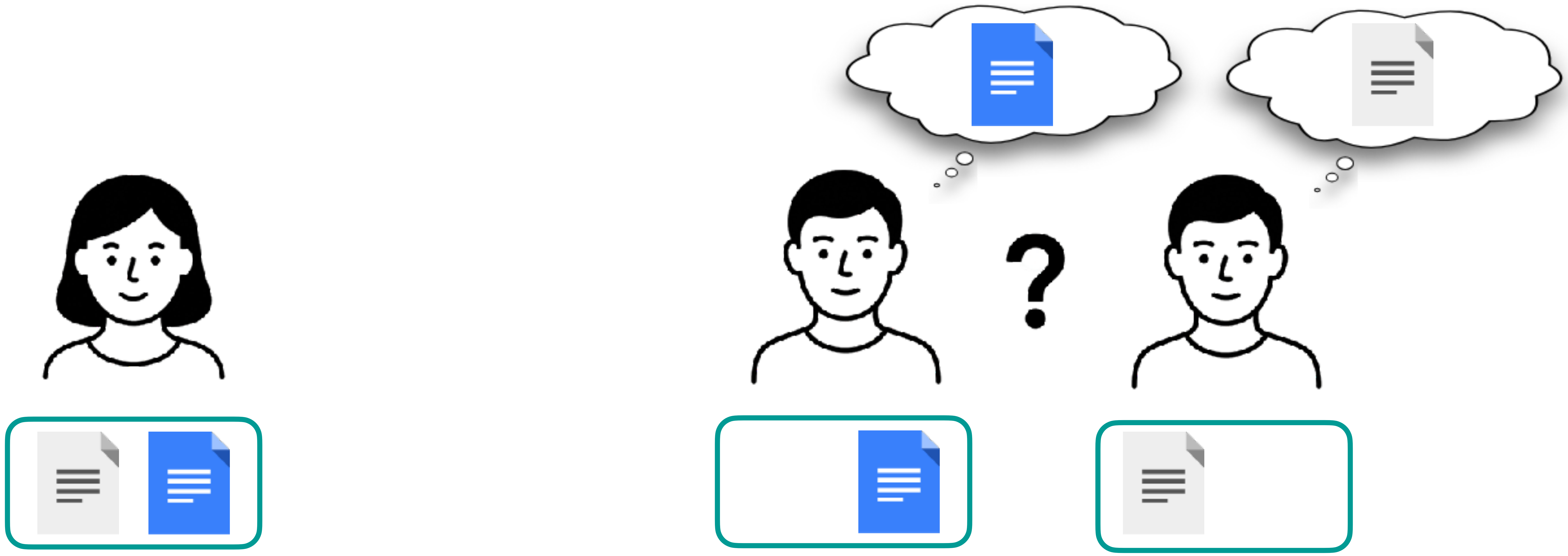
Transfert Inconscient



- Alice possède deux documents, Bob veut apprendre l’un d’entre eux
- Alice souhaite révéler au plus un document
- Bob ne veut pas révéler son choix

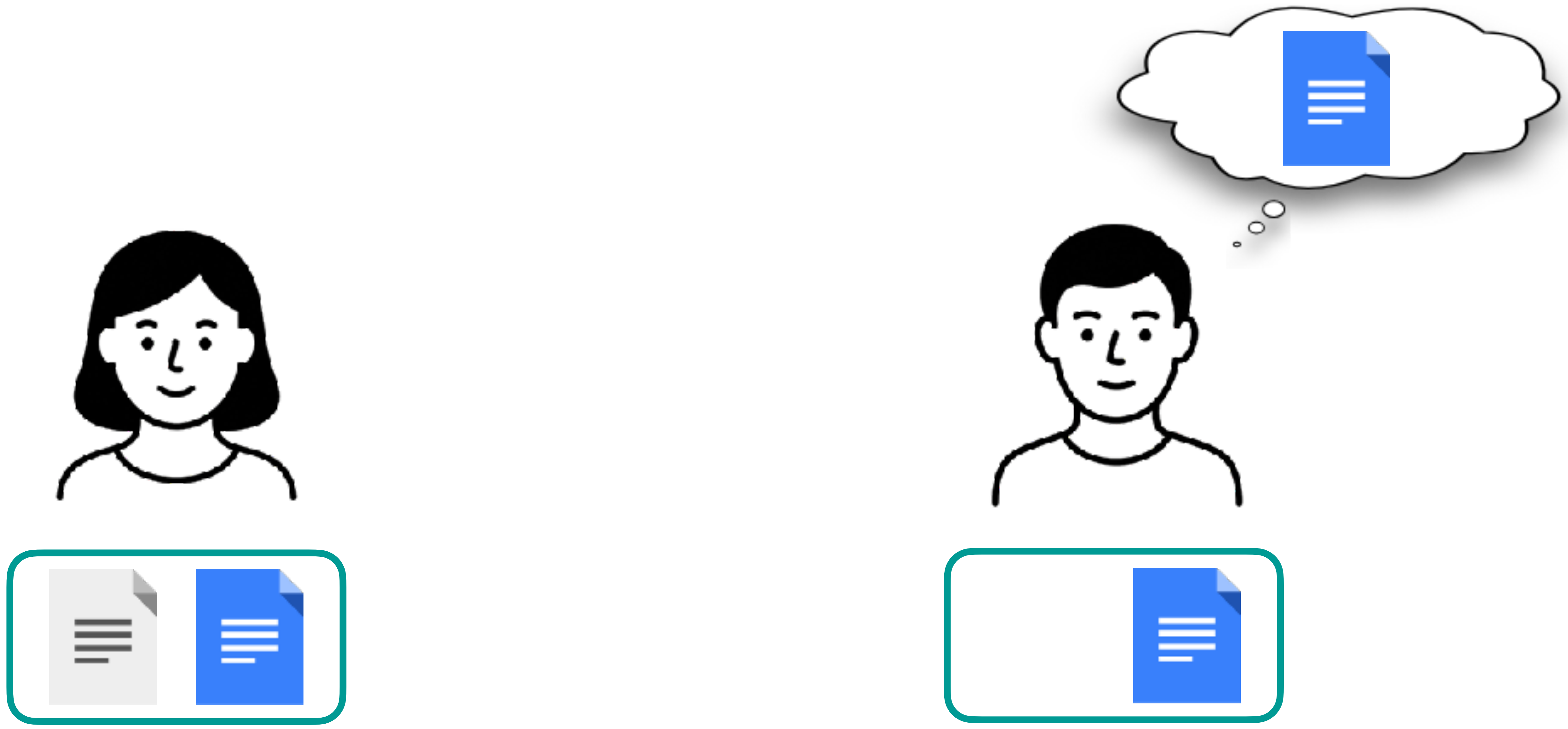
Transfert Inconscient

RAPPEL DE COURS



- Alice possède deux documents, Bob veut apprendre l’un d’entre eux
- Alice souhaite révéler au plus un document
- ▶ Bob ne veut pas révéler son choix

Transfert Inconscient



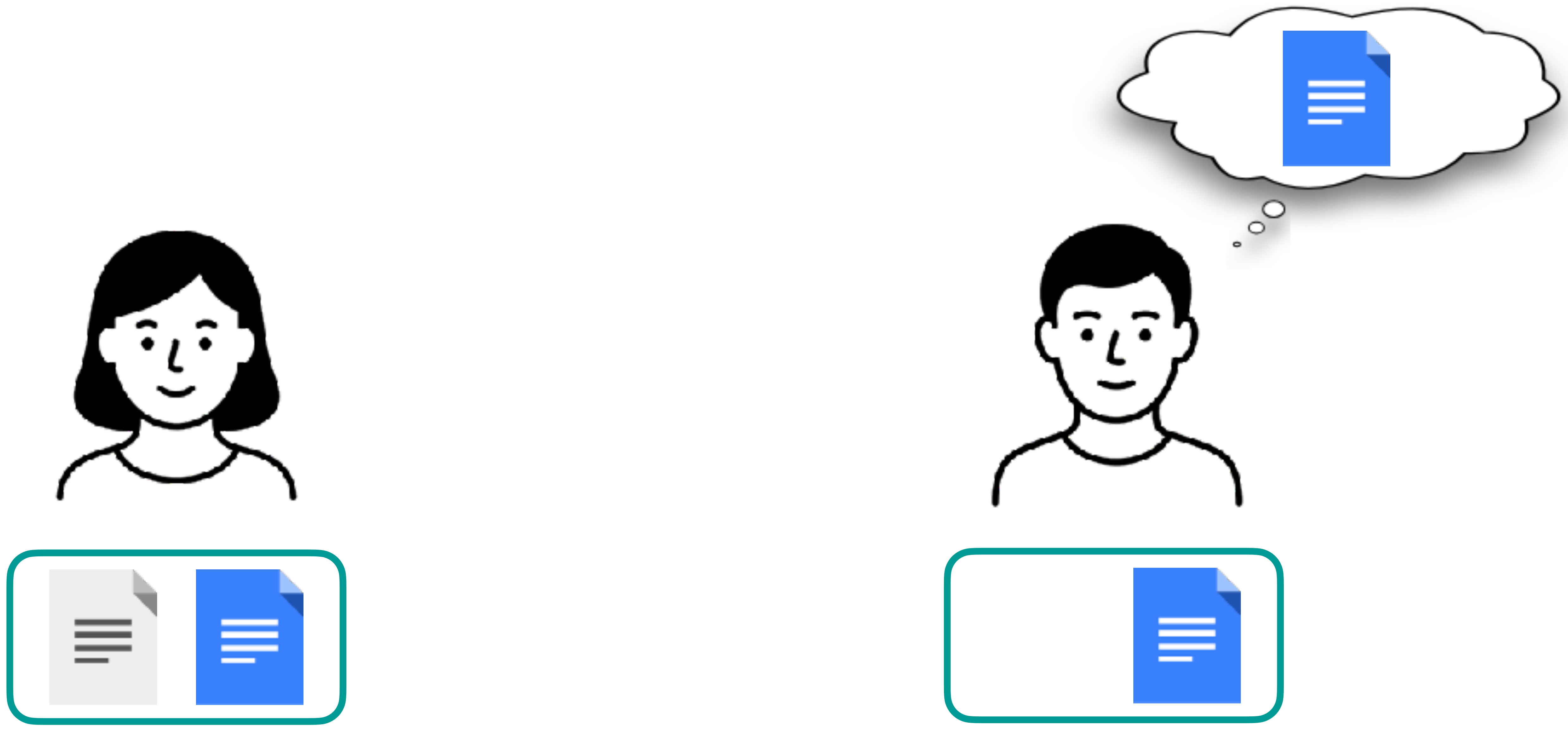
- Alice possède deux documents, Bob veut apprendre l’un d’entre eux
- Alice souhaite révéler au plus un document
- ► Bob ne veut pas révéler son choix

Quel est le coût ?

Construction EGL sous ElGamal,
librairie standard, plate-forme Amazon

Transfert Inconscient

RAPPEL DE COURS



- Alice possède deux documents, Bob veut apprendre l'un d'entre eux
- Alice souhaite révéler au plus un document
- ► Bob ne veut pas révéler son choix

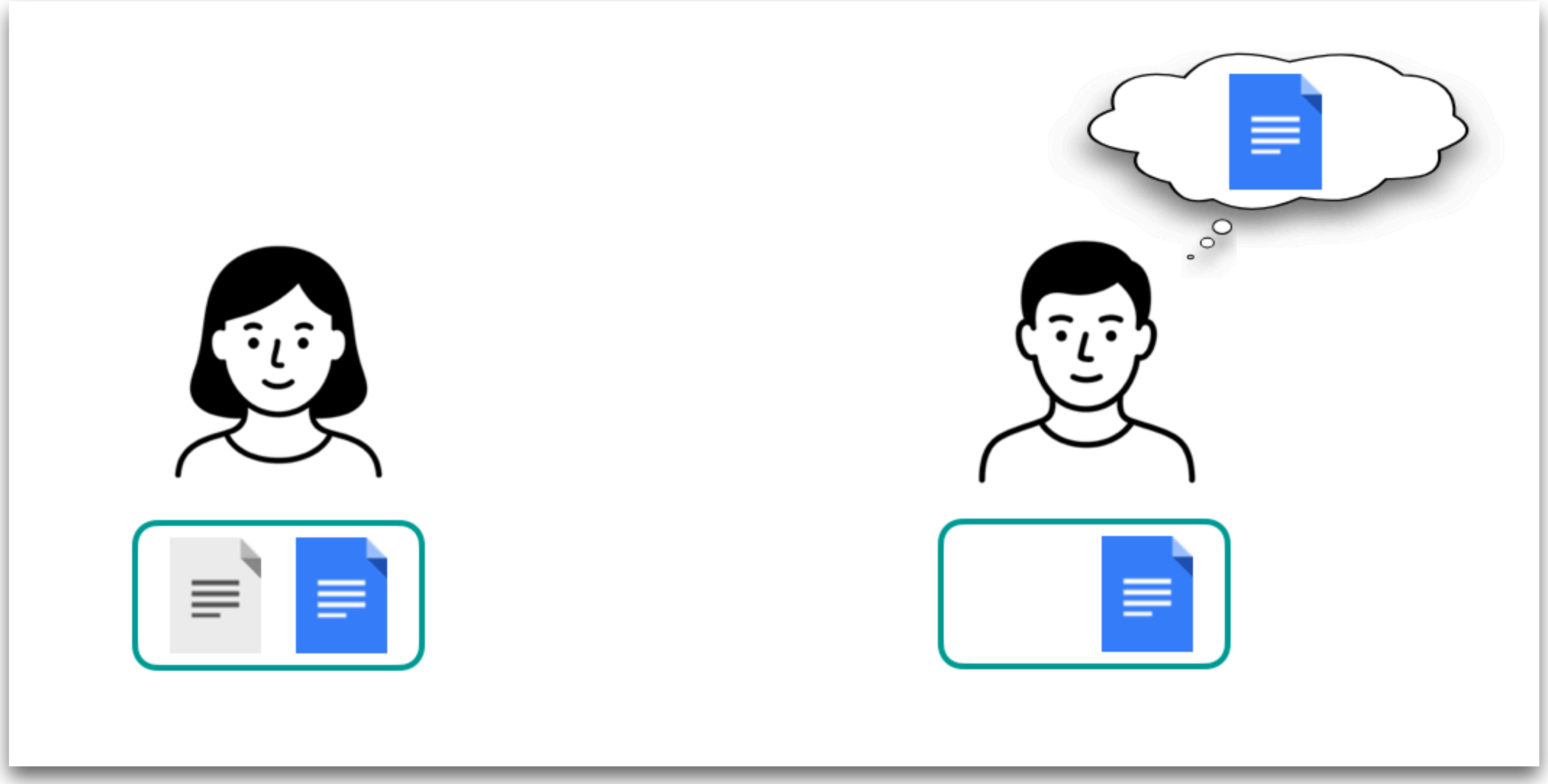
Quel est le coût ?

Construction EGL sous ElGamal, librairie standard, plate-forme Amazon →

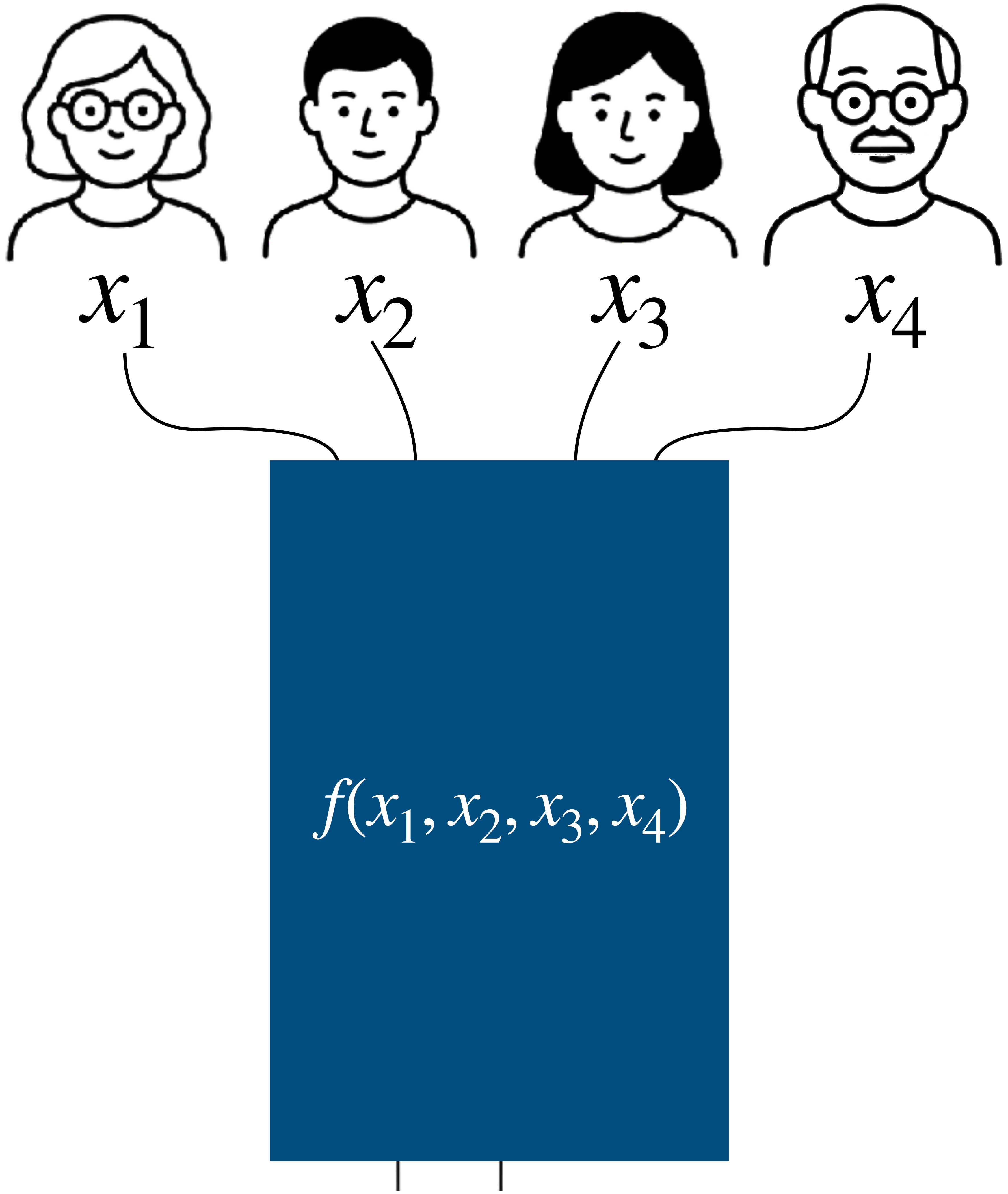
: 250 us

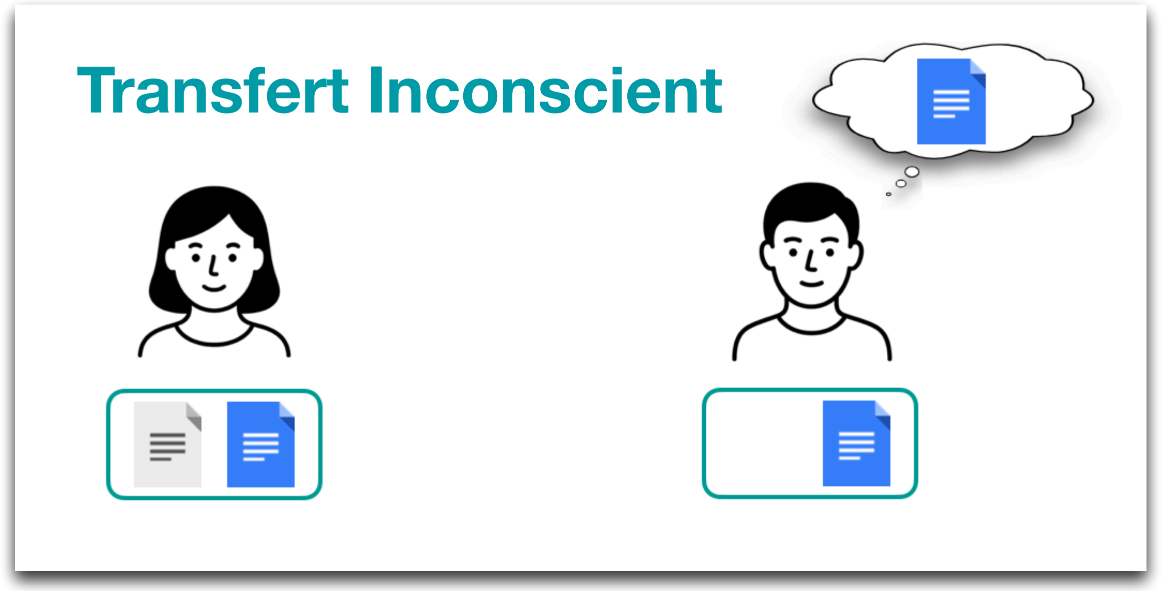
: 128 octets

Calcul sécurisé



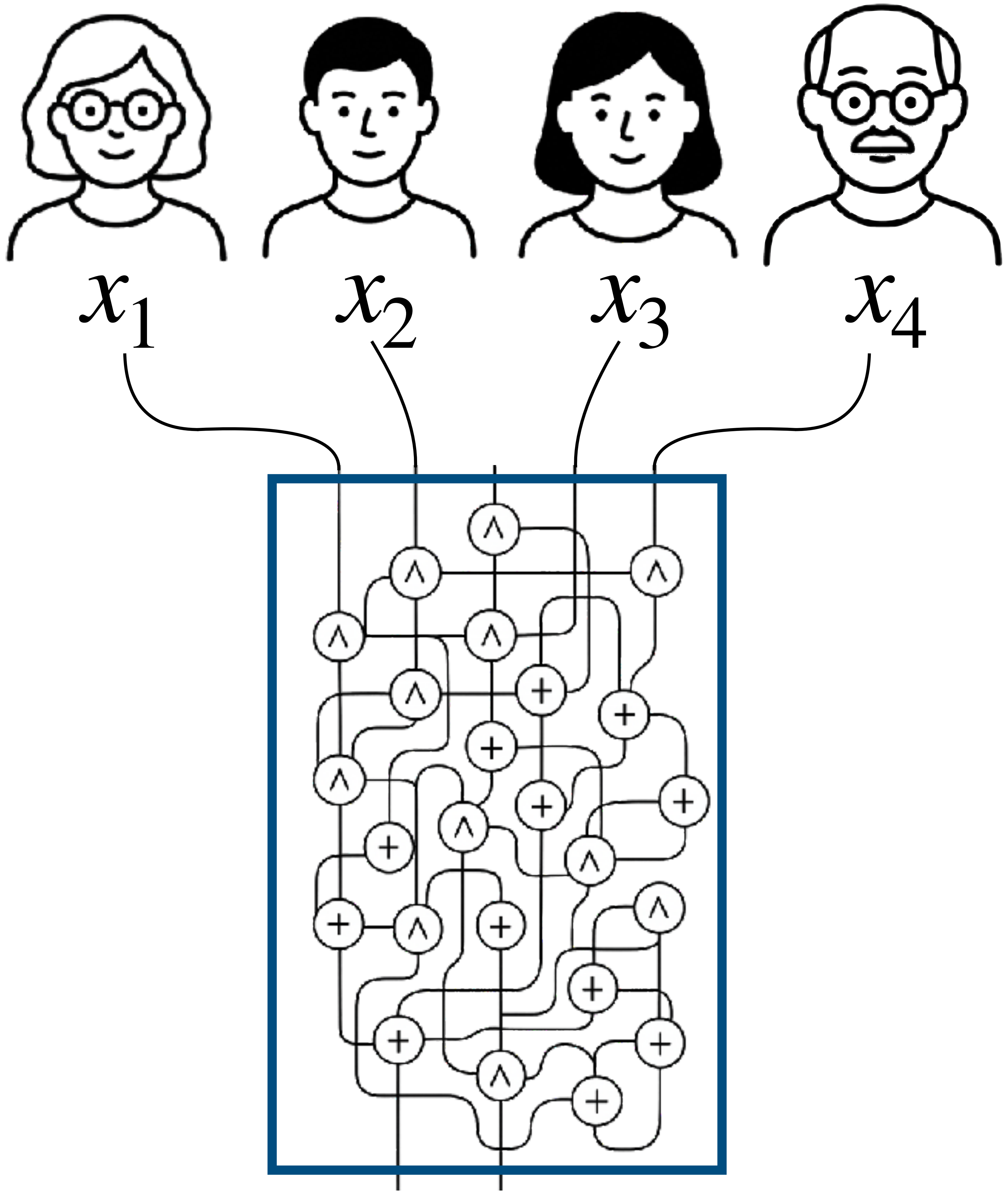
Calcul sécurisé

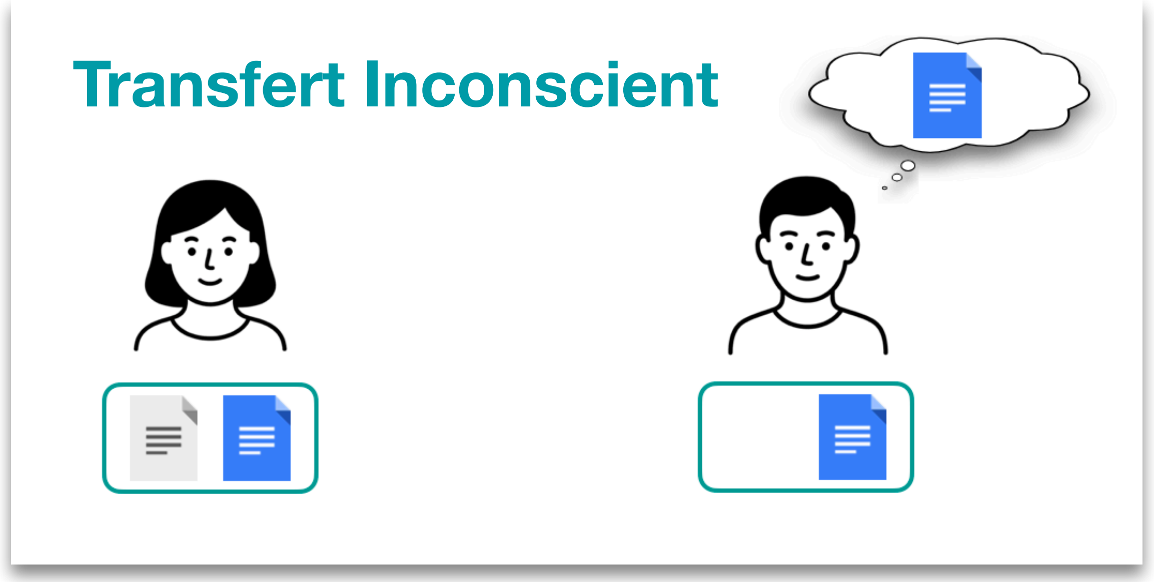




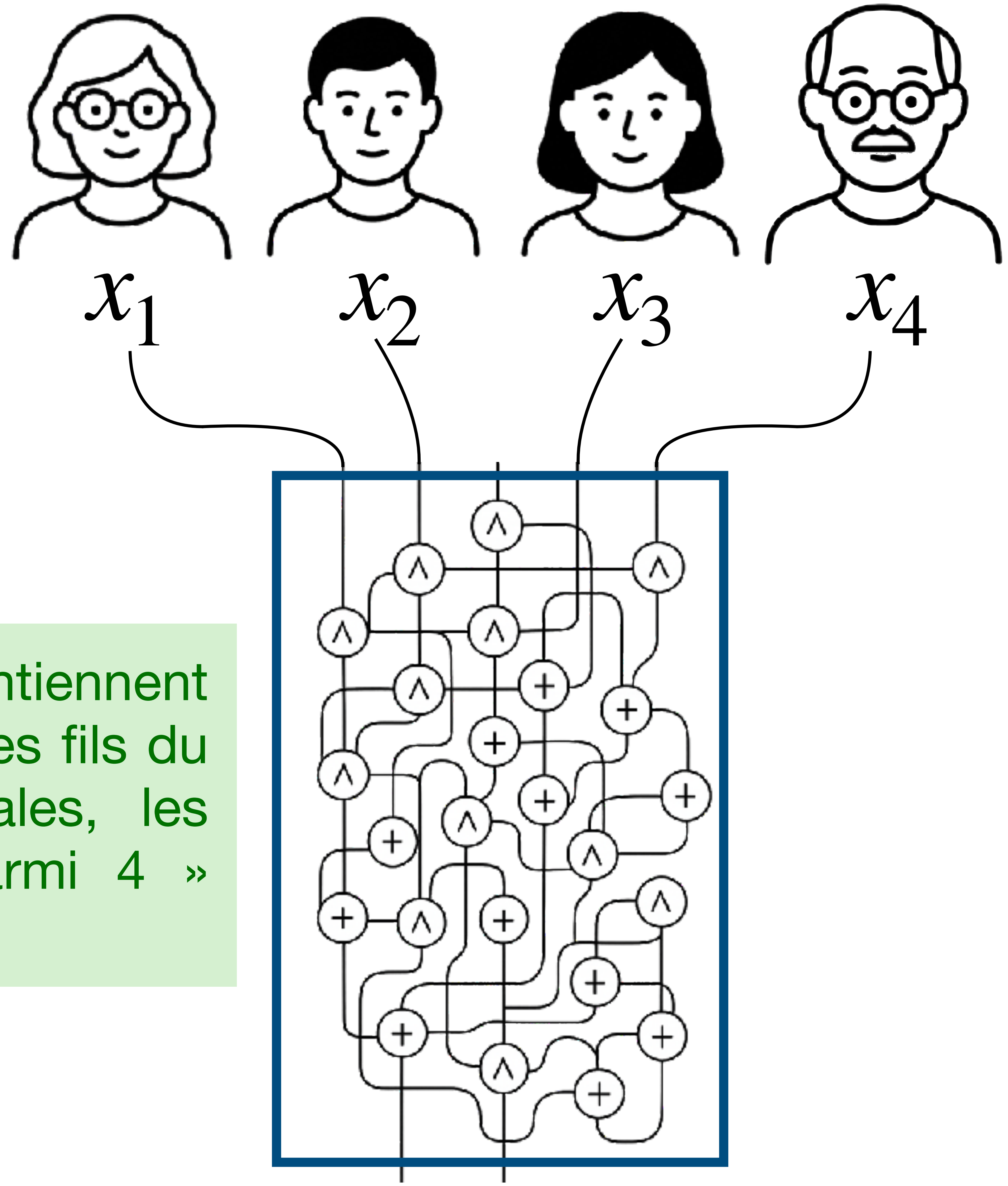
Calcul sécurisé via le protocole GMW

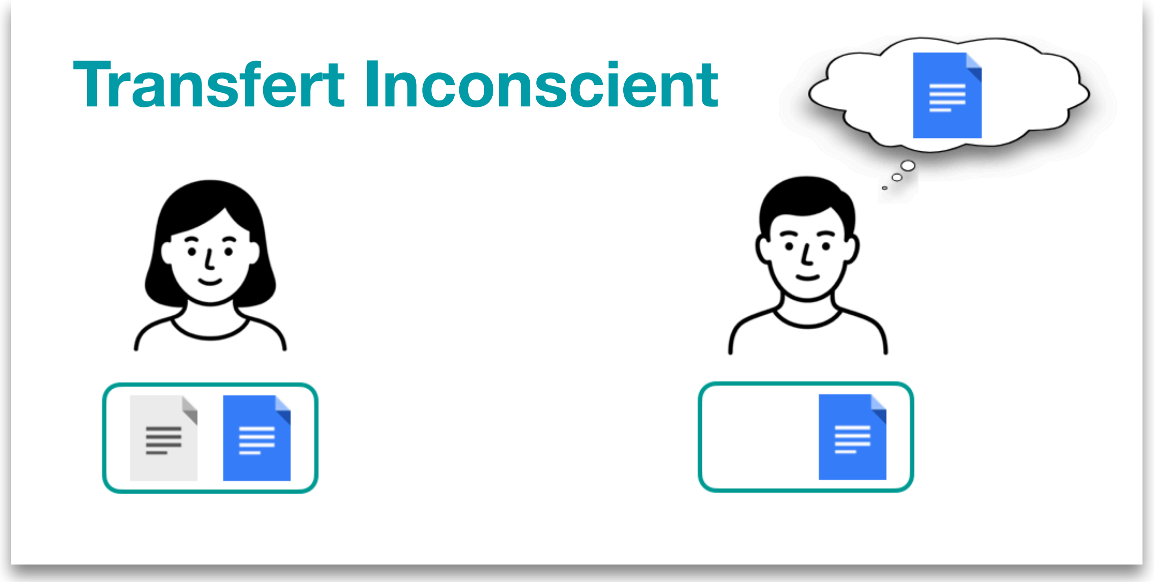
RAPPEL DE COURS





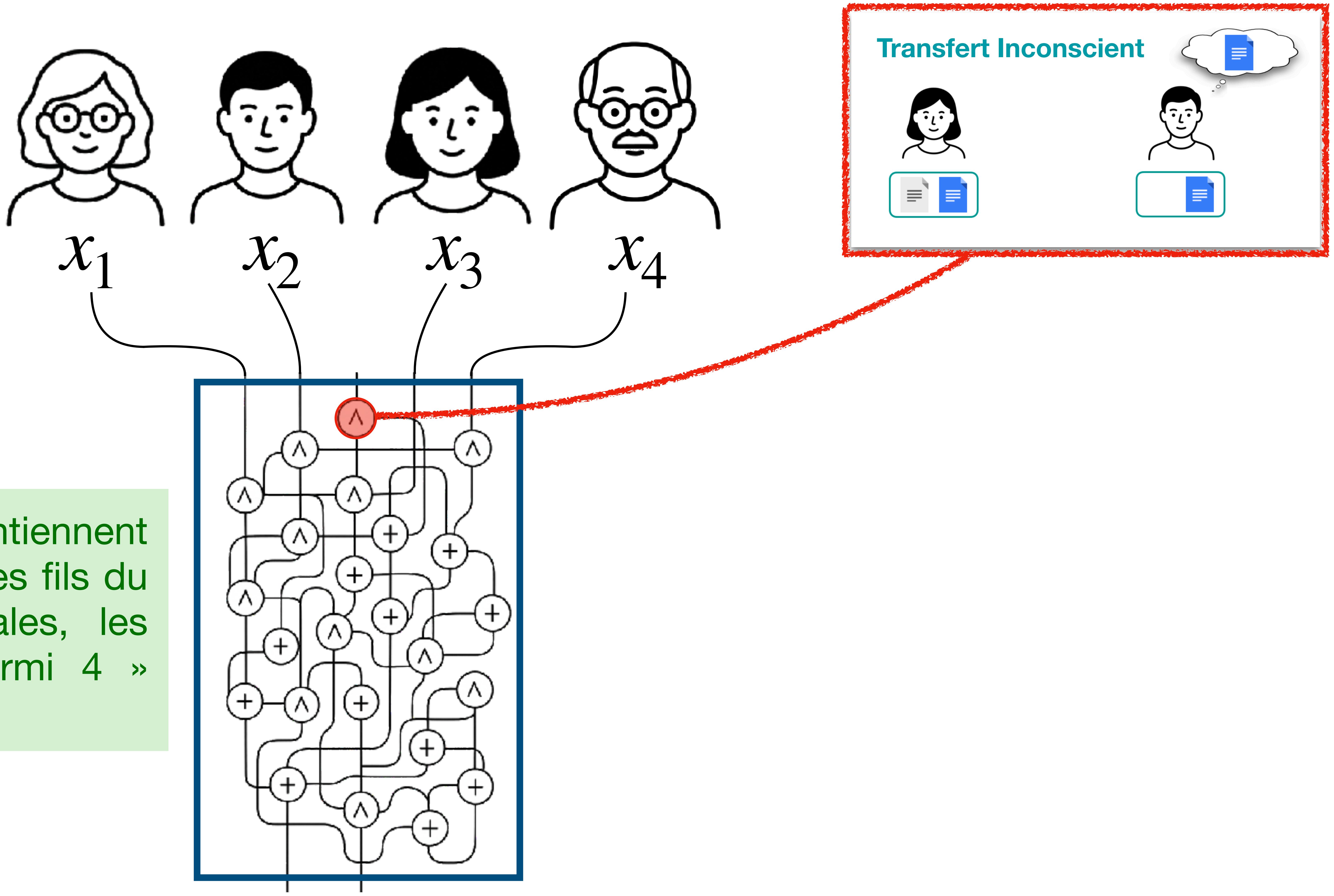
Calcul sécurisé via le protocole GMW





Cf cours. Rappel : les joueurs maintiennent des parts des valeurs transitant sur les fils du circuit. Les portes XOR sont locales, les portes ET utilisent un OT « 1 parmi 4 » (faisable en deux OT « 1 parmi 2 »)

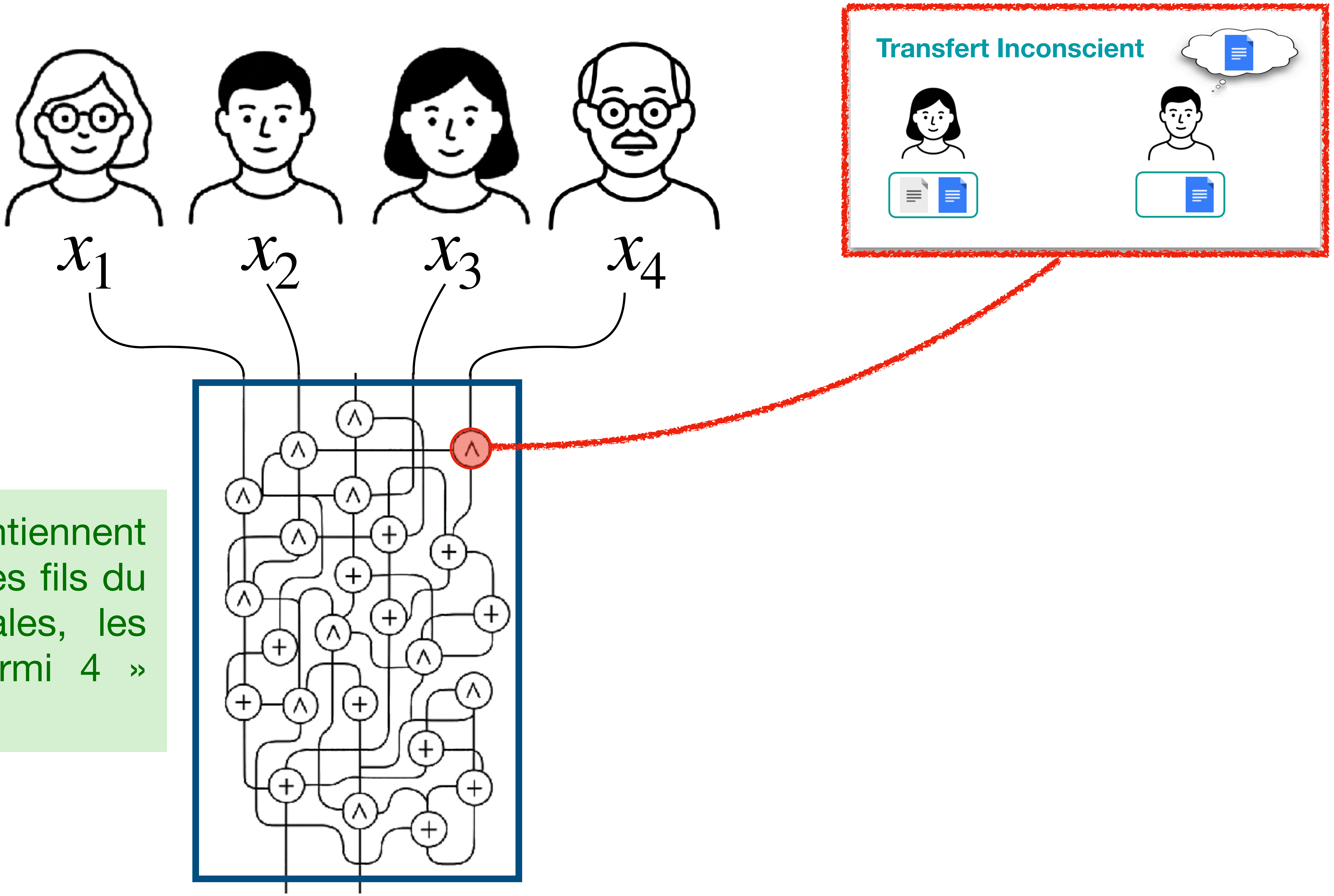
Calcul sécurisé via le protocole GMW



Cf cours. Rappel : les joueurs maintiennent des parts des valeurs transitant sur les fils du circuit. Les portes XOR sont locales, les portes ET utilisent un OT « 1 parmi 4 » (faisable en deux OT « 1 parmi 2 »)

Calcul sécurisé via le protocole GMW

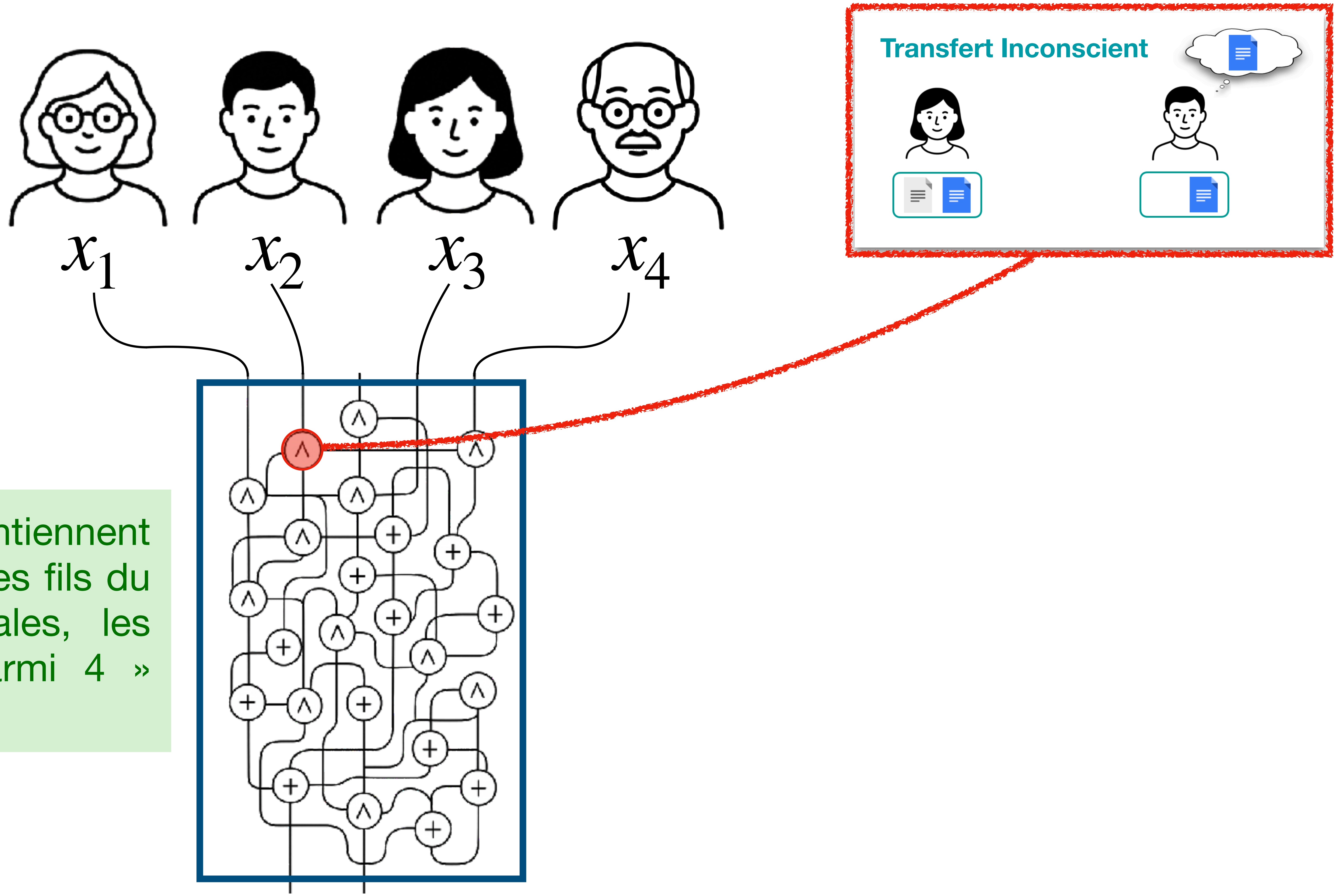
RAPPEL DE COURS



Cf cours. Rappel : les joueurs maintiennent des parts des valeurs transitant sur les fils du circuit. Les portes XOR sont locales, les portes ET utilisent un OT « 1 parmi 4 » (faisable en deux OT « 1 parmi 2 »)

Calcul sécurisé via le protocole GMW

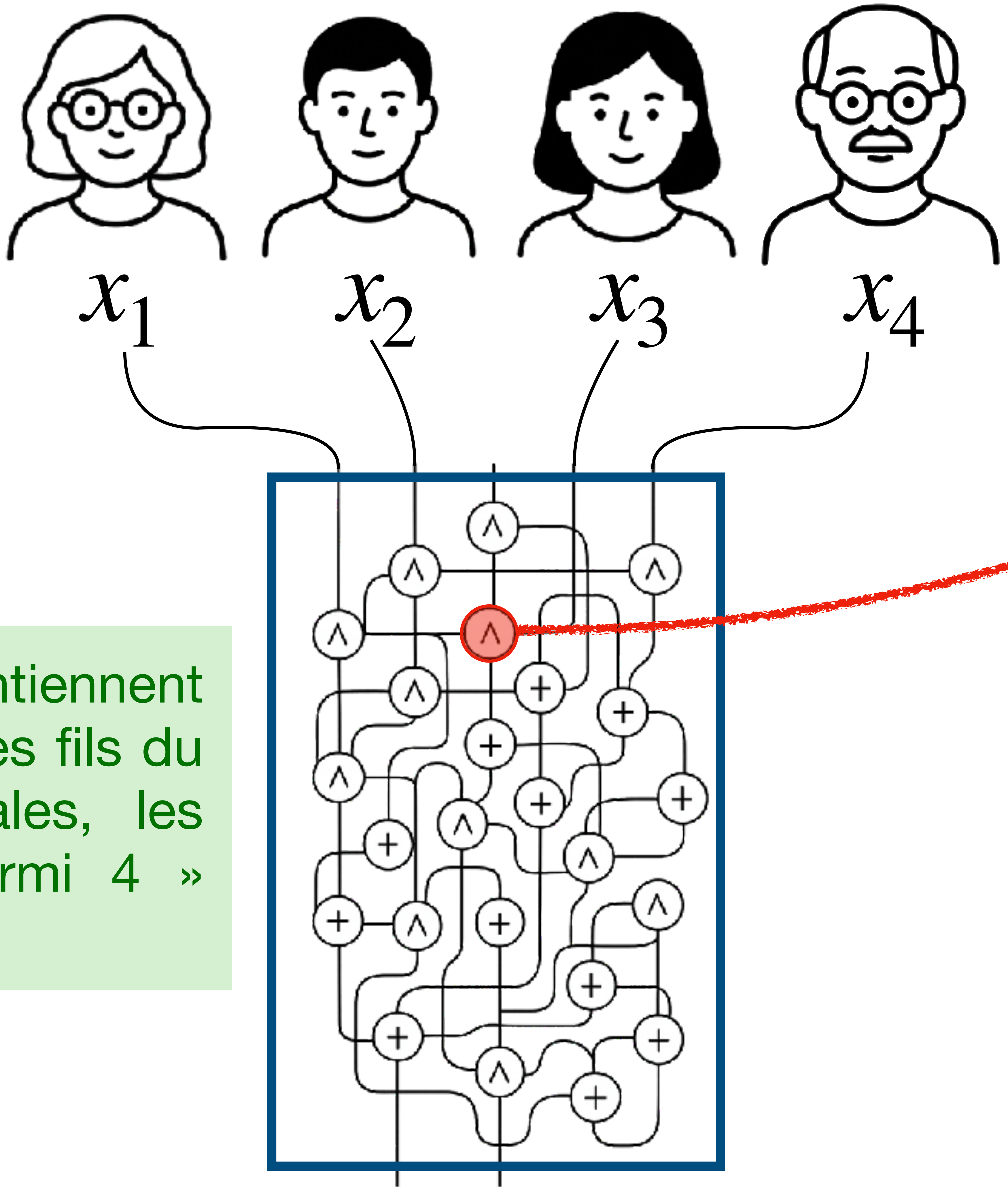
RAPPEL DE COURS

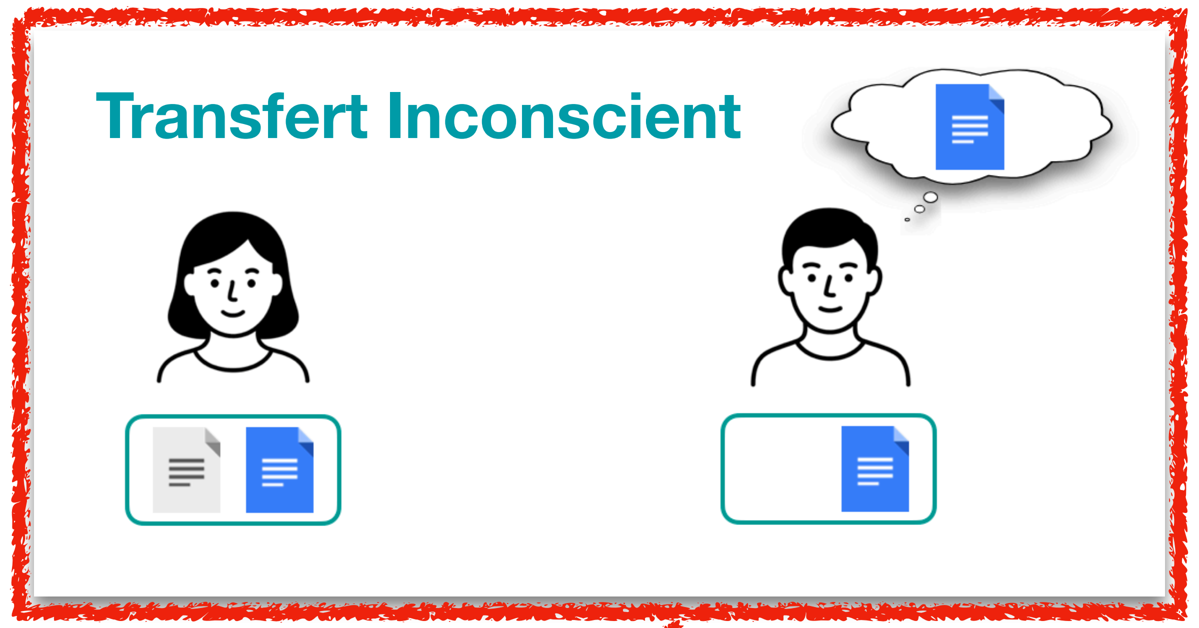


Cf cours. Rappel : les joueurs maintiennent des parts des valeurs transitant sur les fils du circuit. Les portes XOR sont locales, les portes ET utilisent un OT « 1 parmi 4 » (faisable en deux OT « 1 parmi 2 »)

Calcul sécurisé via le protocole GMW

RAPPEL DE COURS

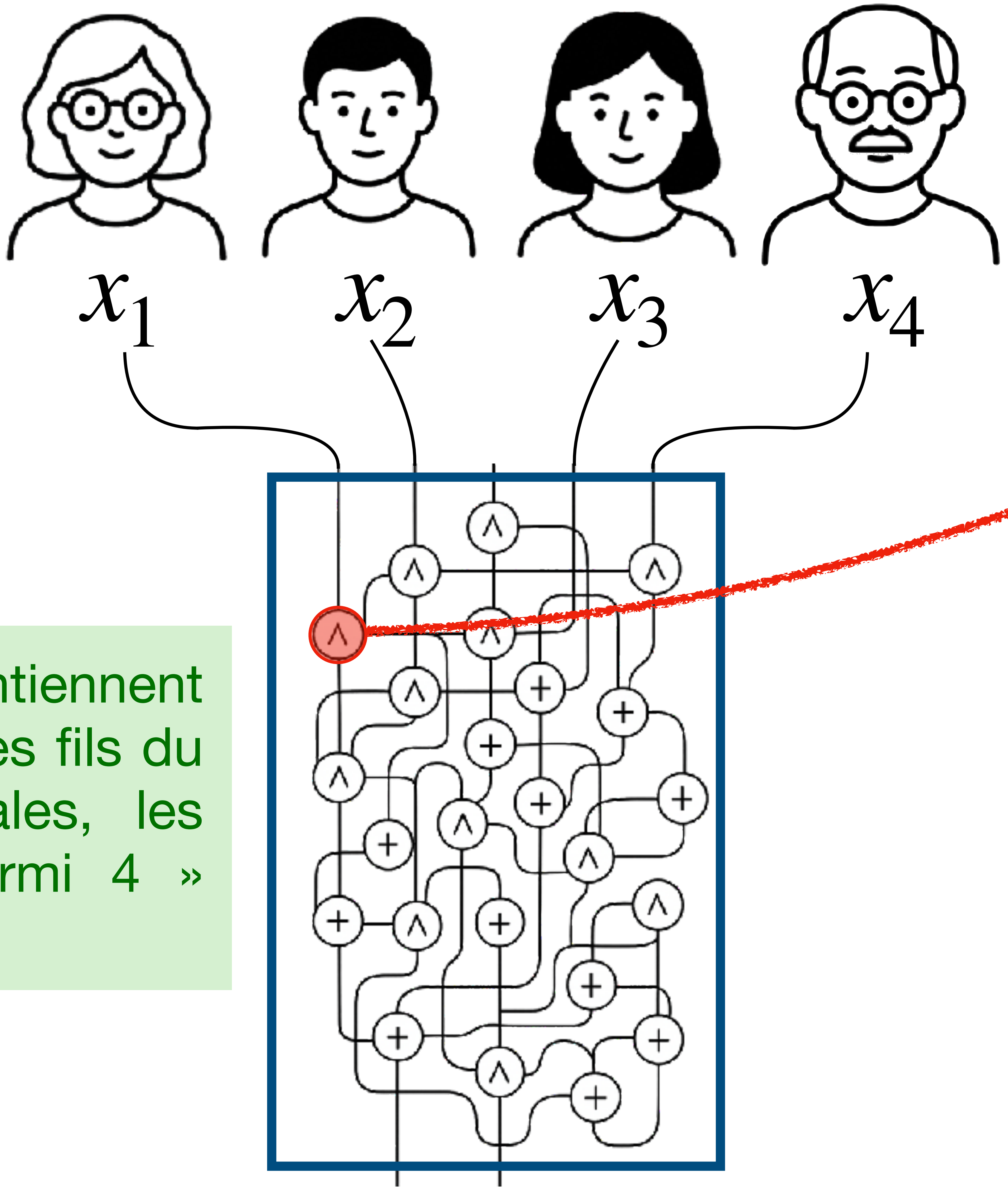


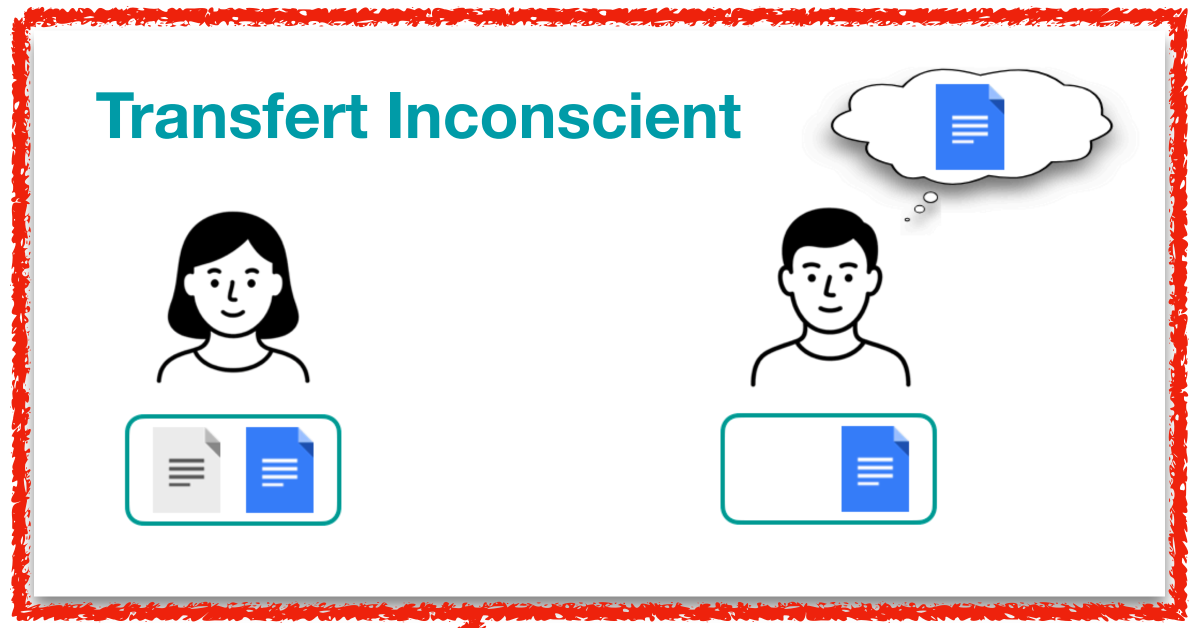


Cf cours. Rappel : les joueurs maintiennent des parts des valeurs transitant sur les fils du circuit. Les portes XOR sont locales, les portes ET utilisent un OT « 1 parmi 4 » (faisable en deux OT « 1 parmi 2 »)

Calcul sécurisé via le protocole GMW

RAPPEL DE COURS

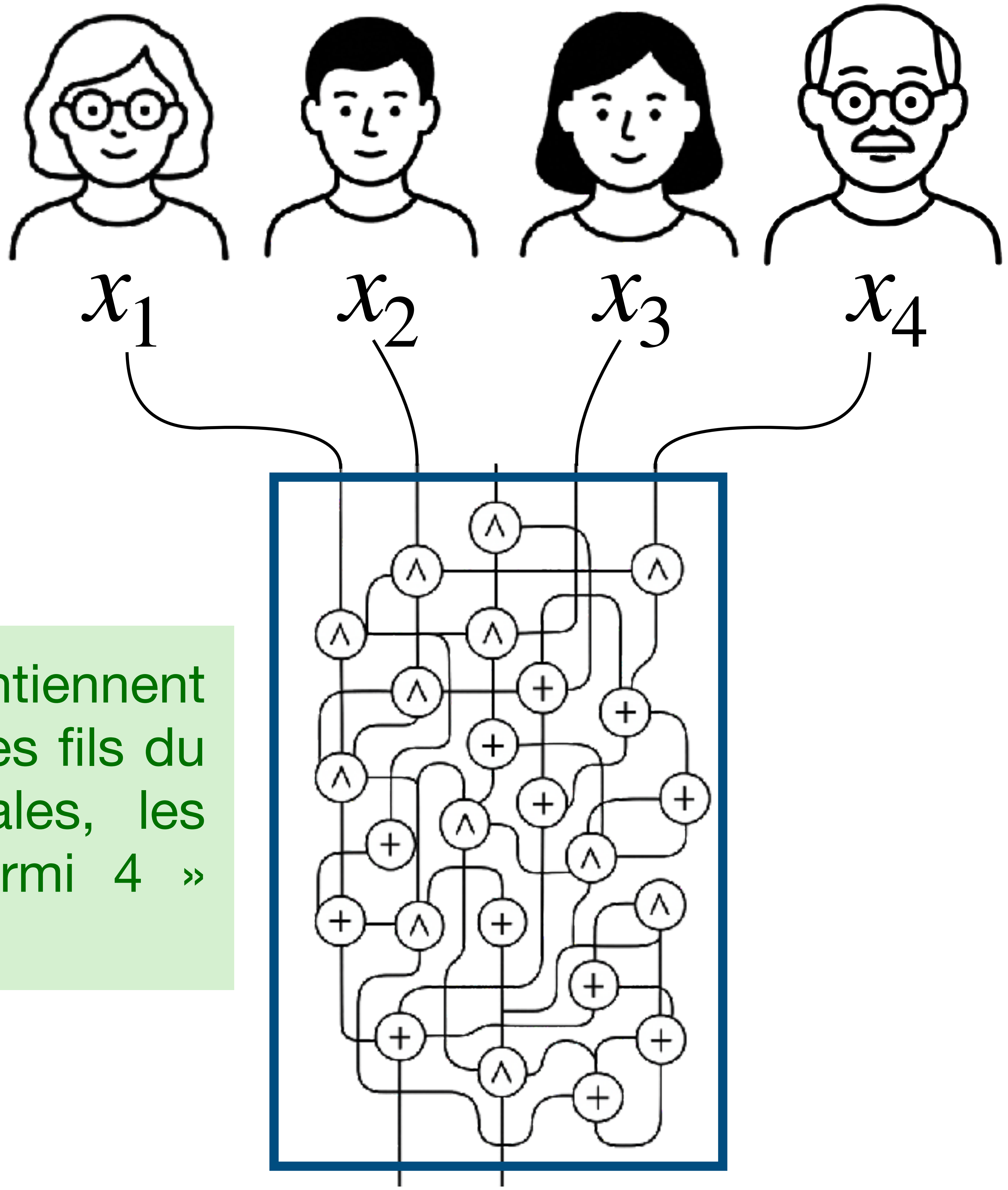




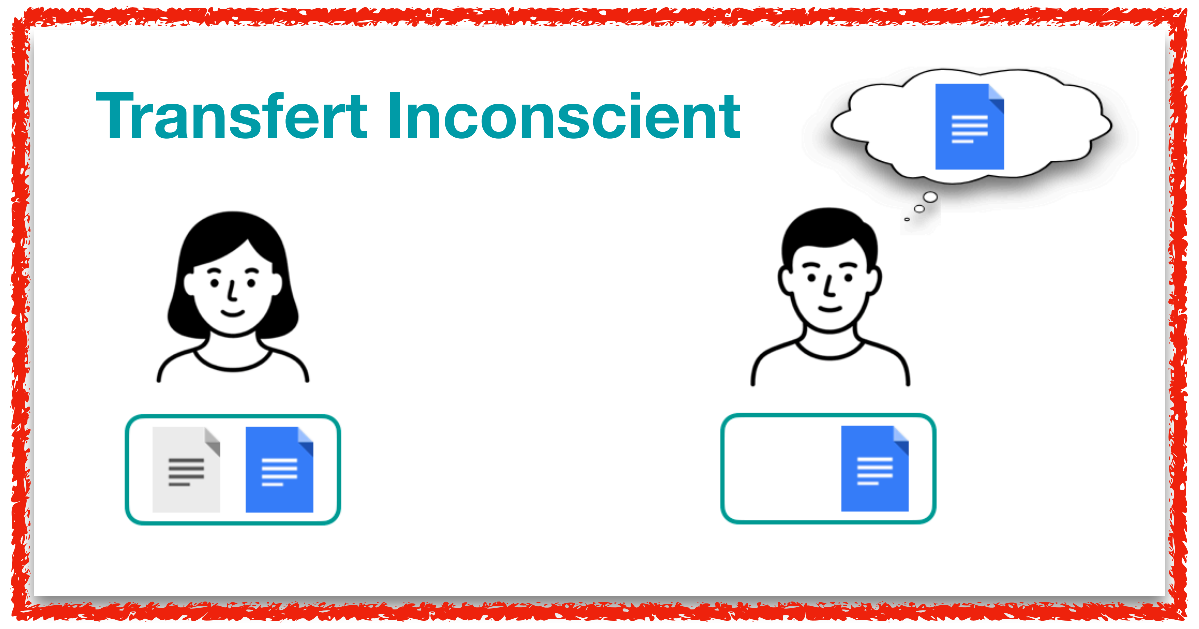
Cf cours. Rappel : les joueurs maintiennent des parts des valeurs transitant sur les fils du circuit. Les portes XOR sont locales, les portes ET utilisent un OT « 1 parmi 4 » (faisable en deux OT « 1 parmi 2 »)

Calcul sécurisé via le protocole GMW

RAPPEL DE COURS

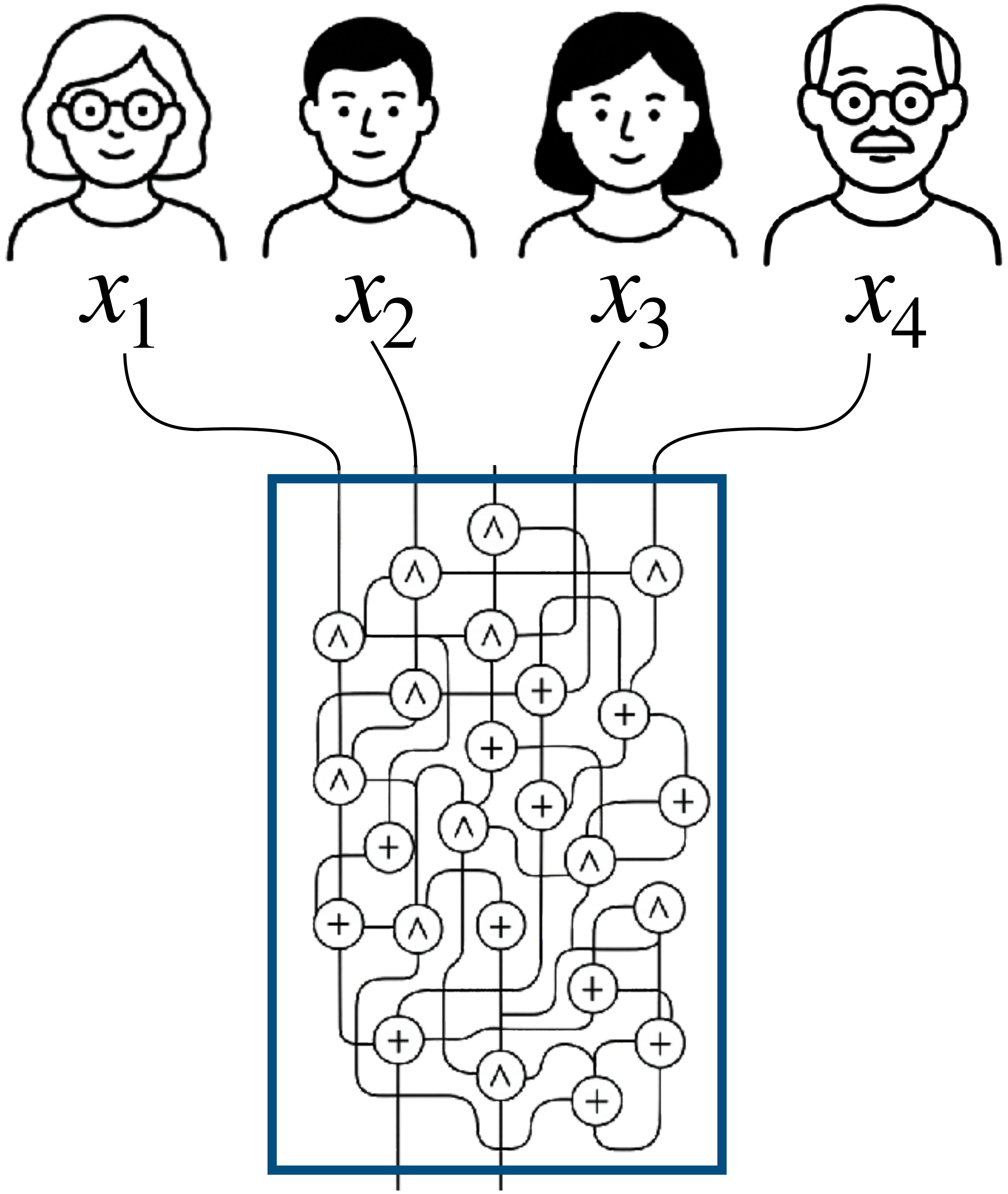


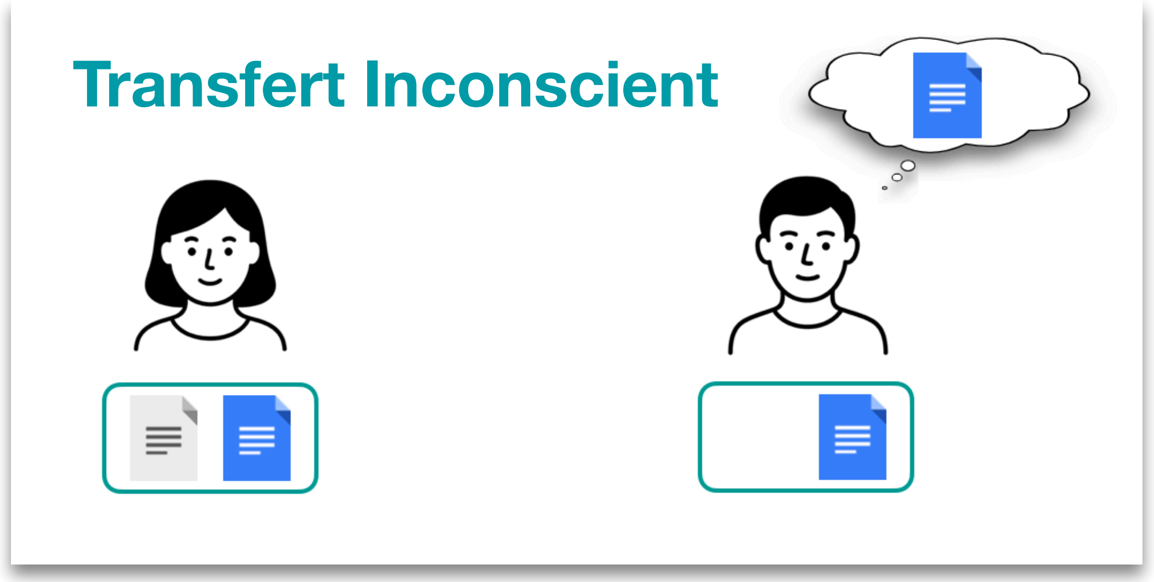
...



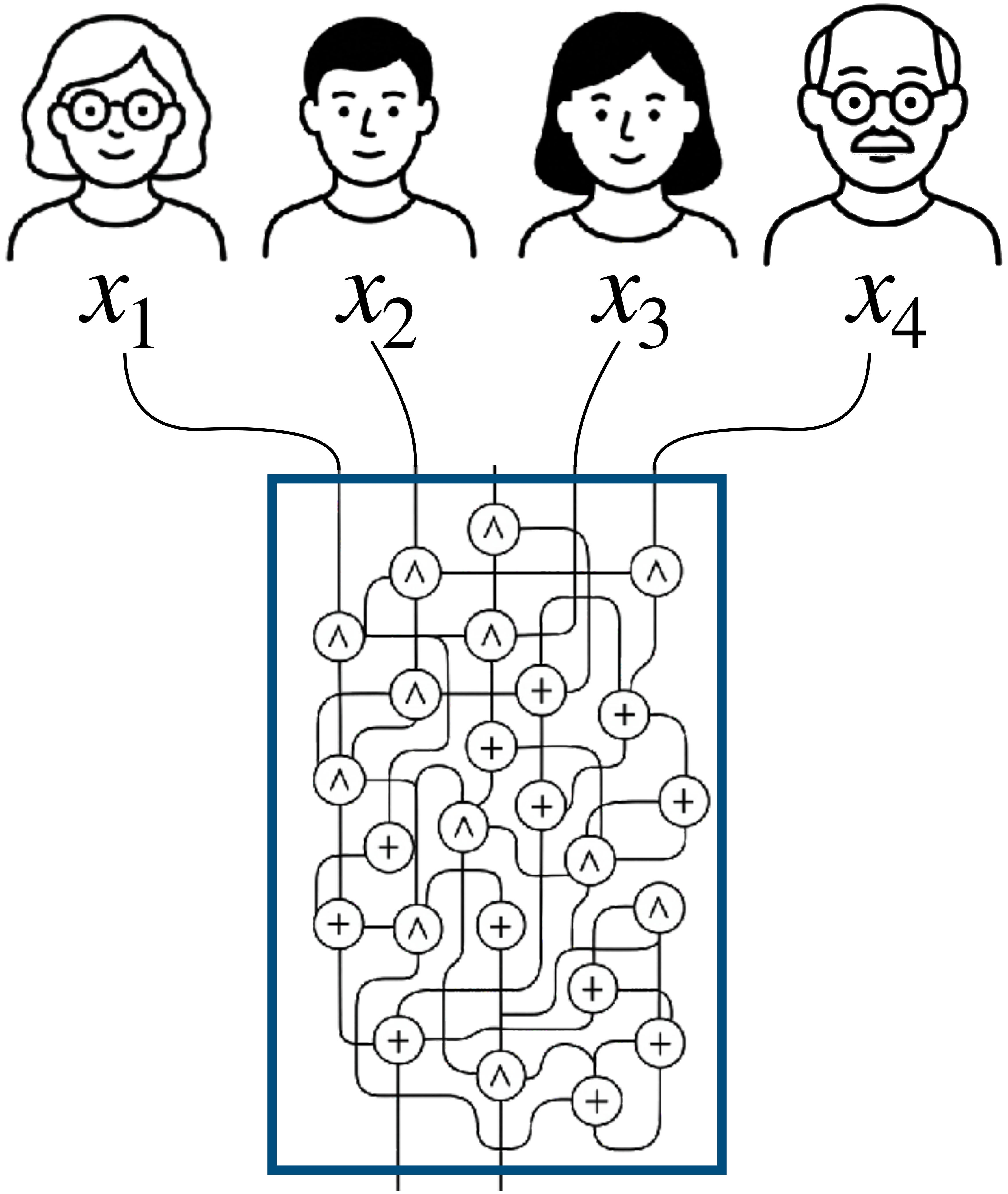
Cf cours. Rappel : les joueurs maintiennent des parts des valeurs transitant sur les fils du circuit. Les portes XOR sont locales, les portes ET utilisent un OT « 1 parmi 4 » (faisable en deux OT « 1 parmi 2 »)

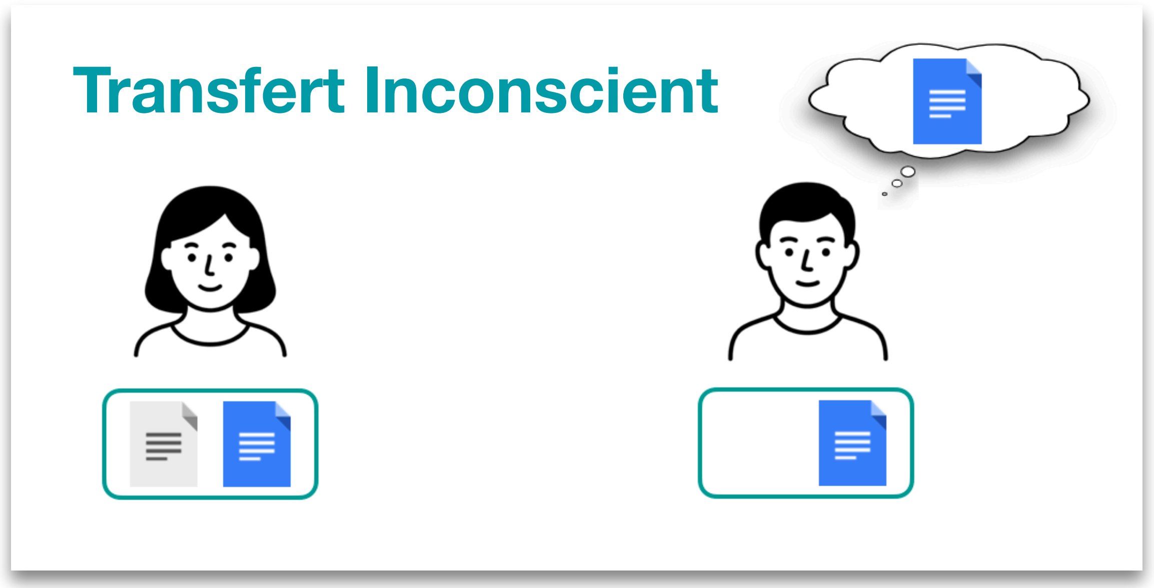
Calcul sécurisé via le protocole GMW



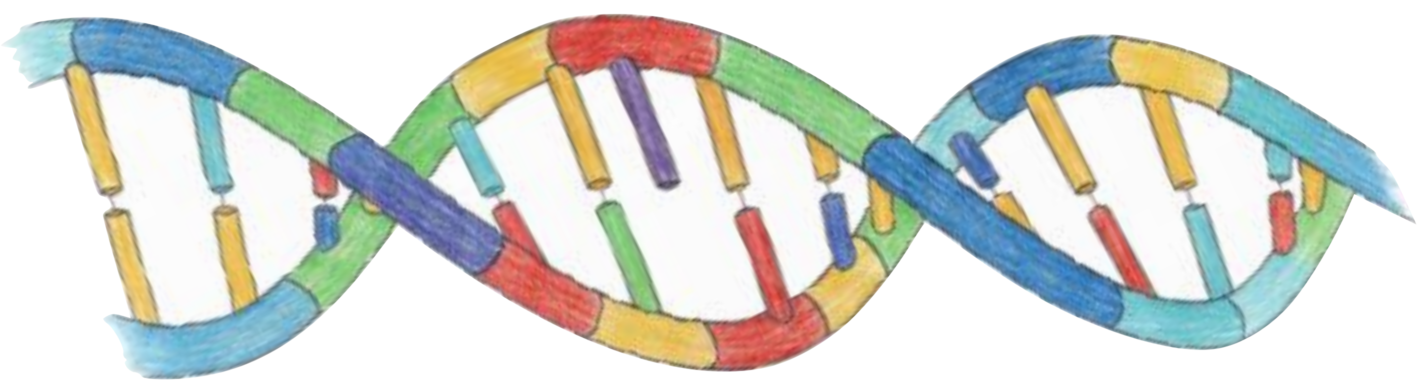


Calcul sécurisé via le protocole GMW

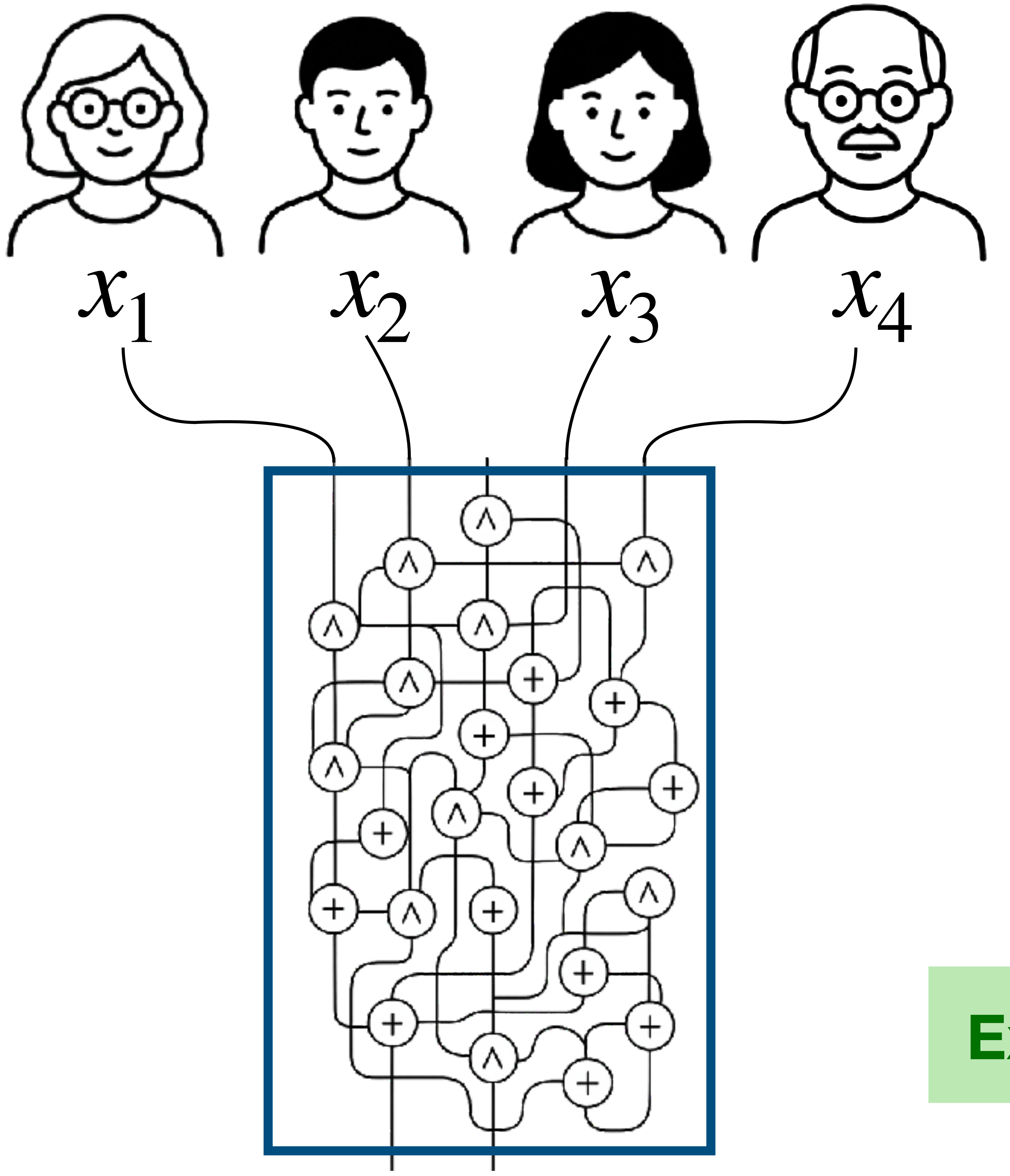


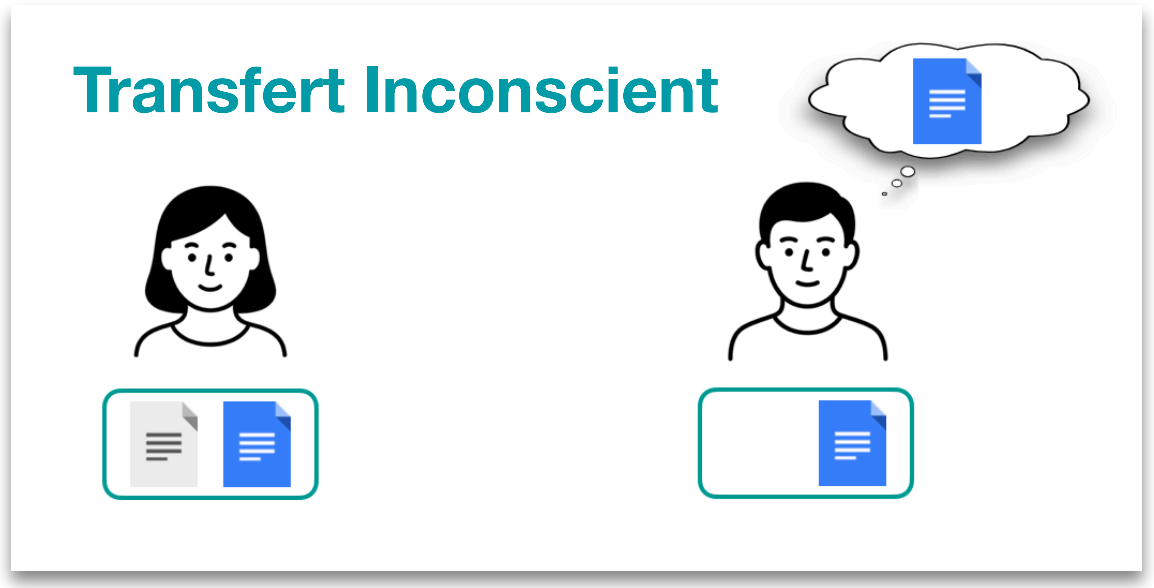


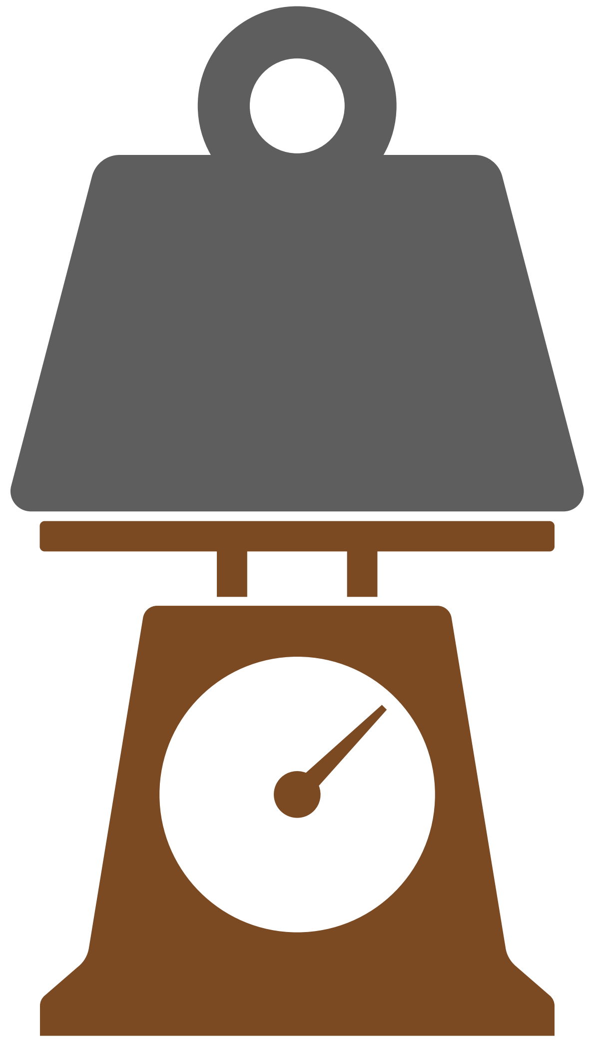
Calcul sécurisé via le protocole GMW



AAACGTACCTGACAAT

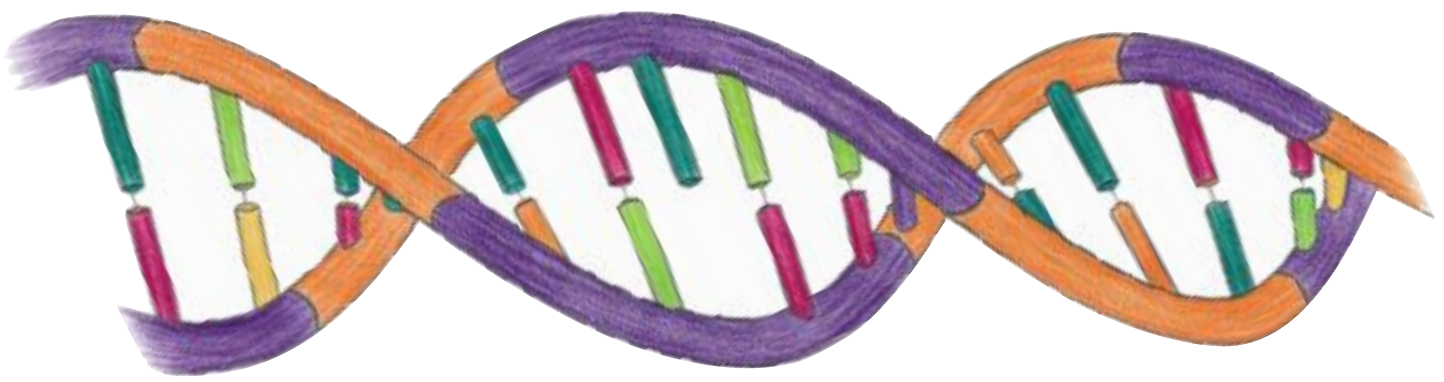




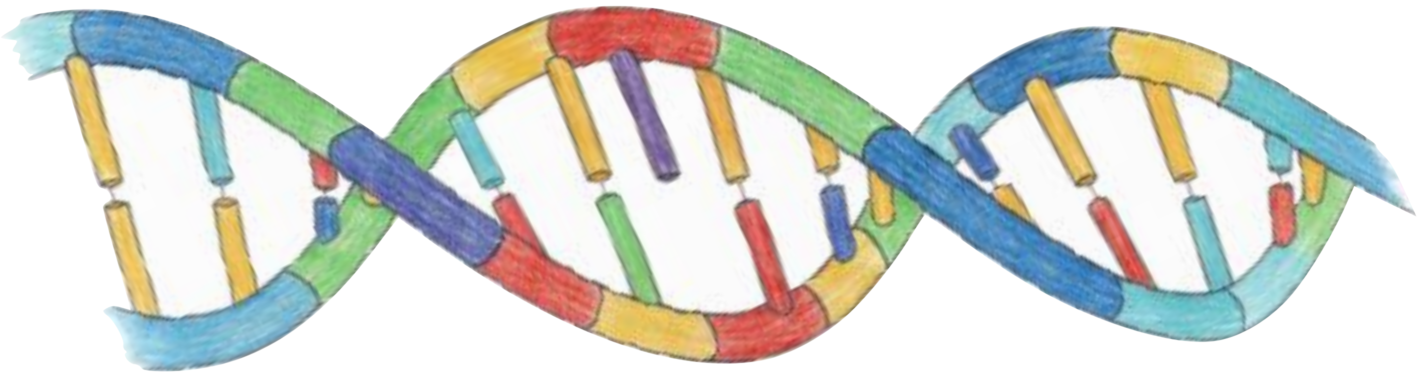


Exemple : distance d'édition

TACGCGTCTTGAGCT

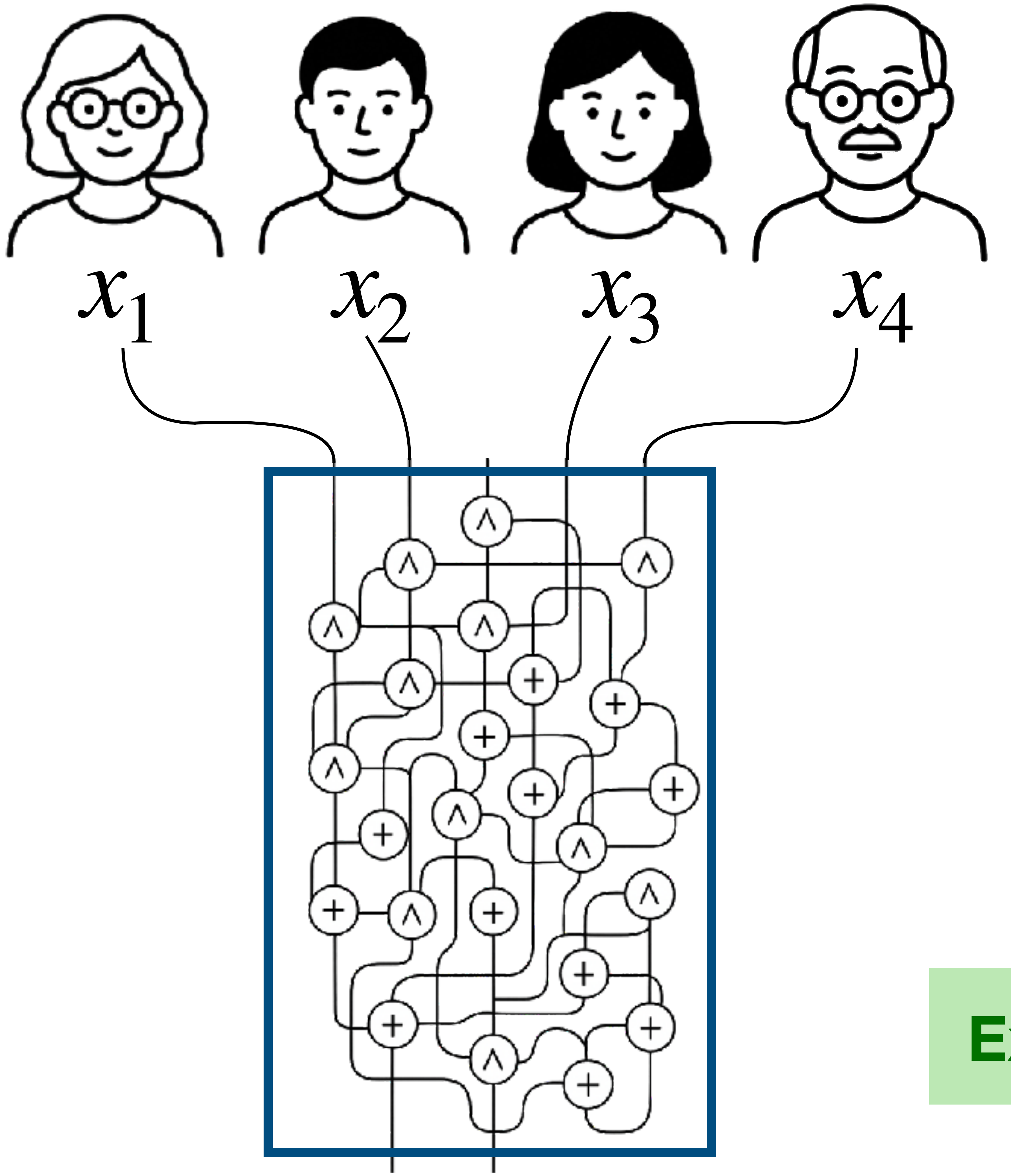


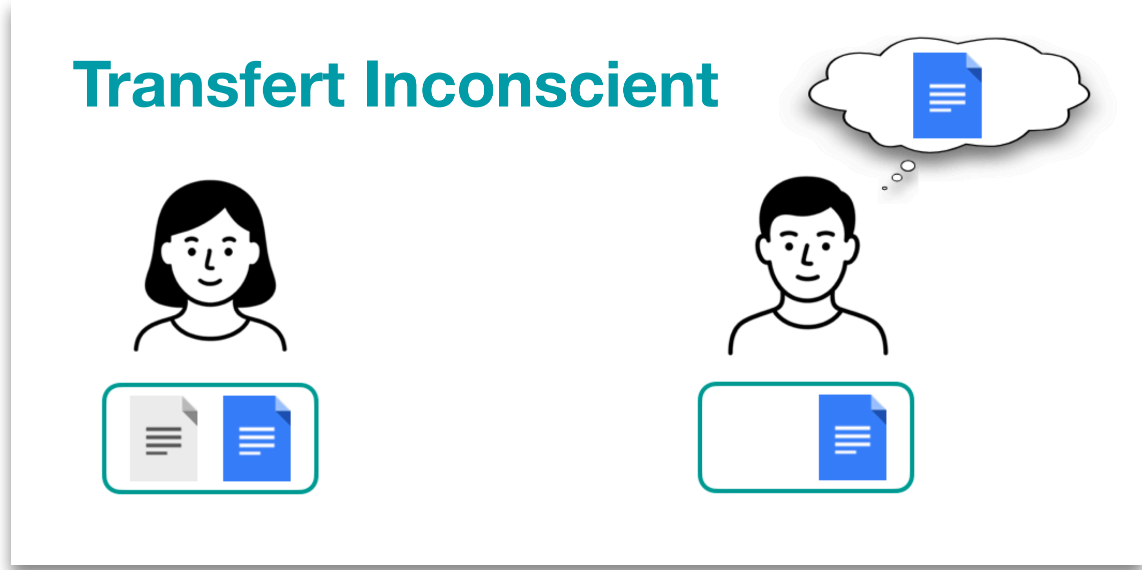
Calcul sécurisé via le protocole GMW

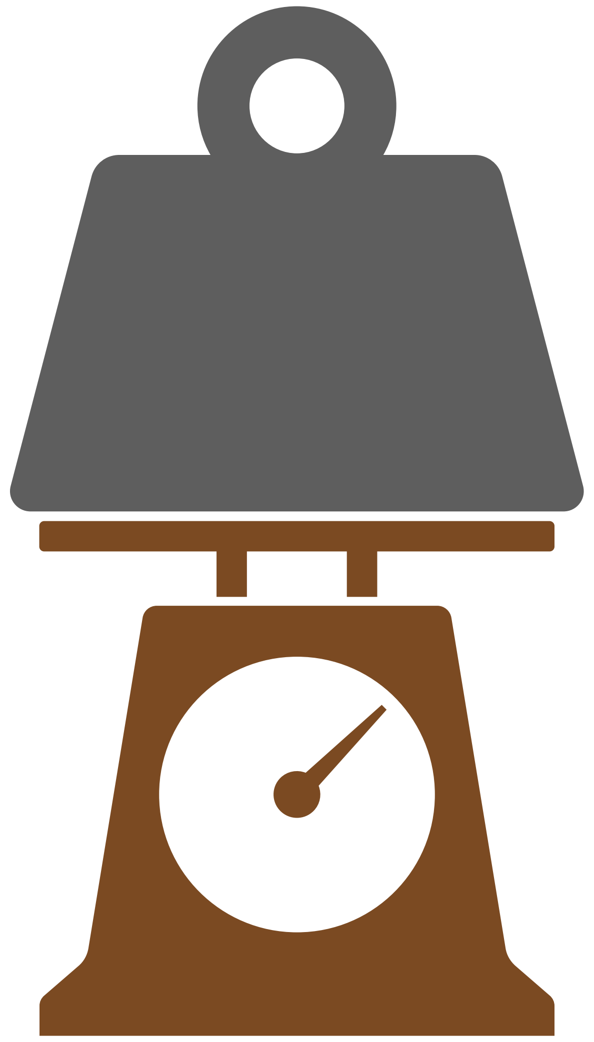


AAACGTACCTGACAAT

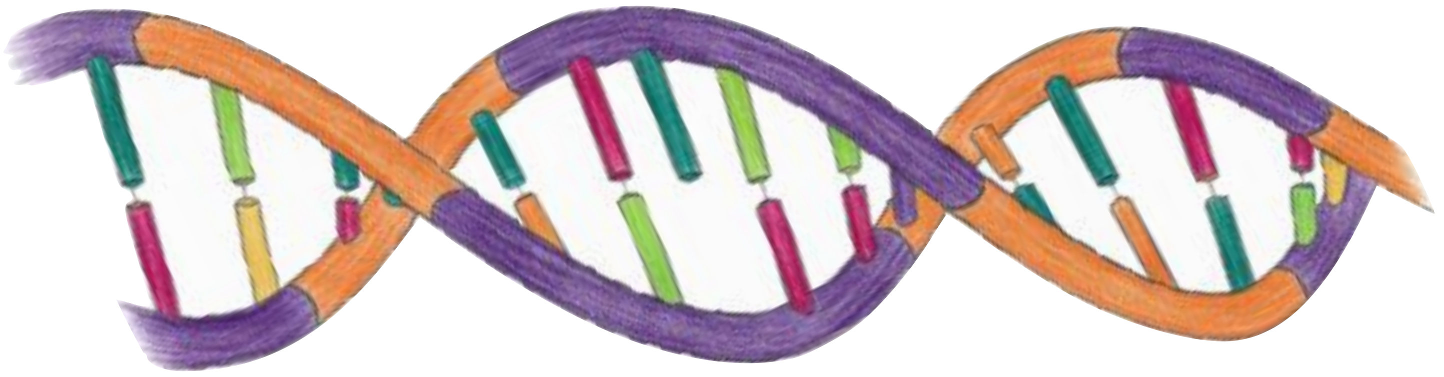
ACACGTACCTGACAAT





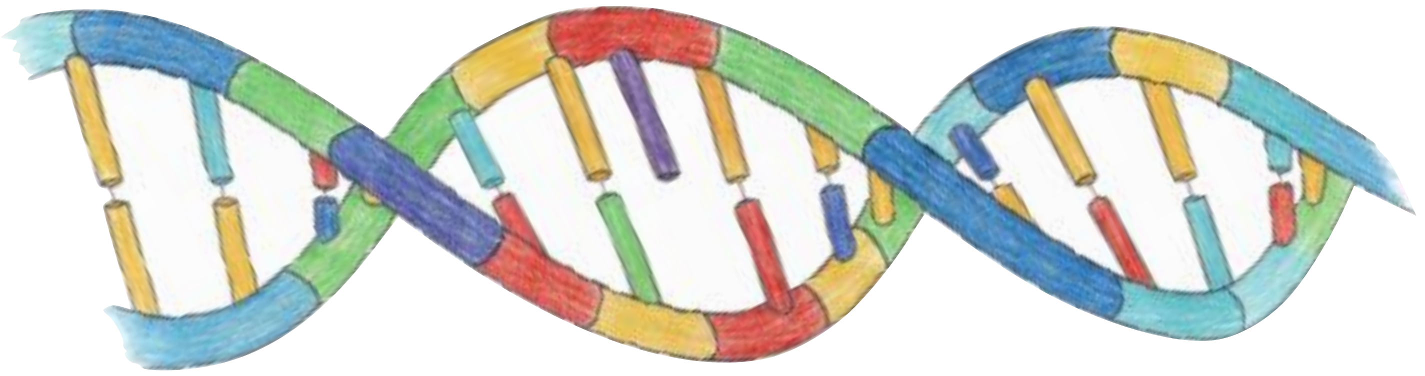


TACGCGTCTTGAGCT



Exemple : distance d'édition

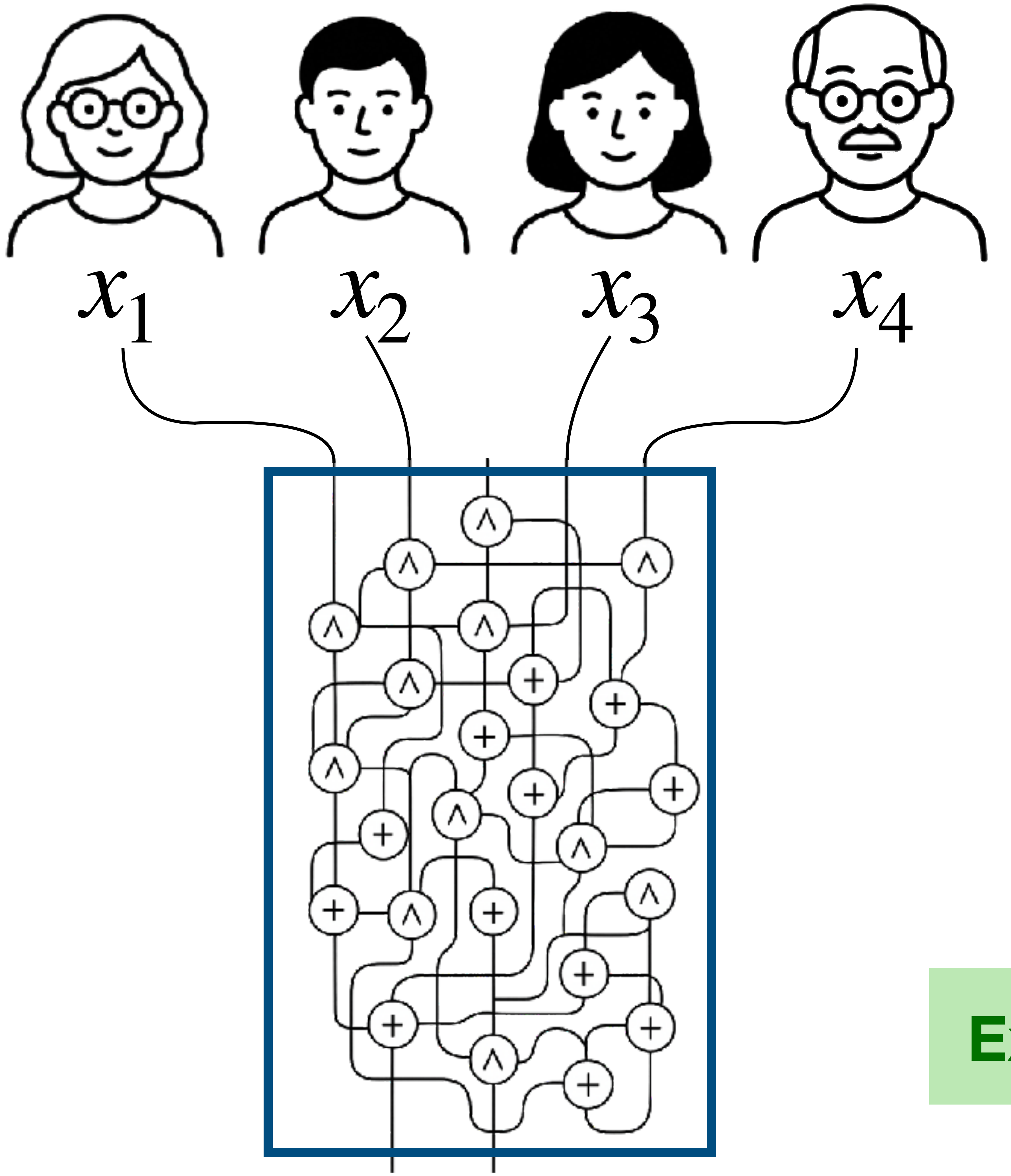
Calcul sécurisé via le protocole GMW

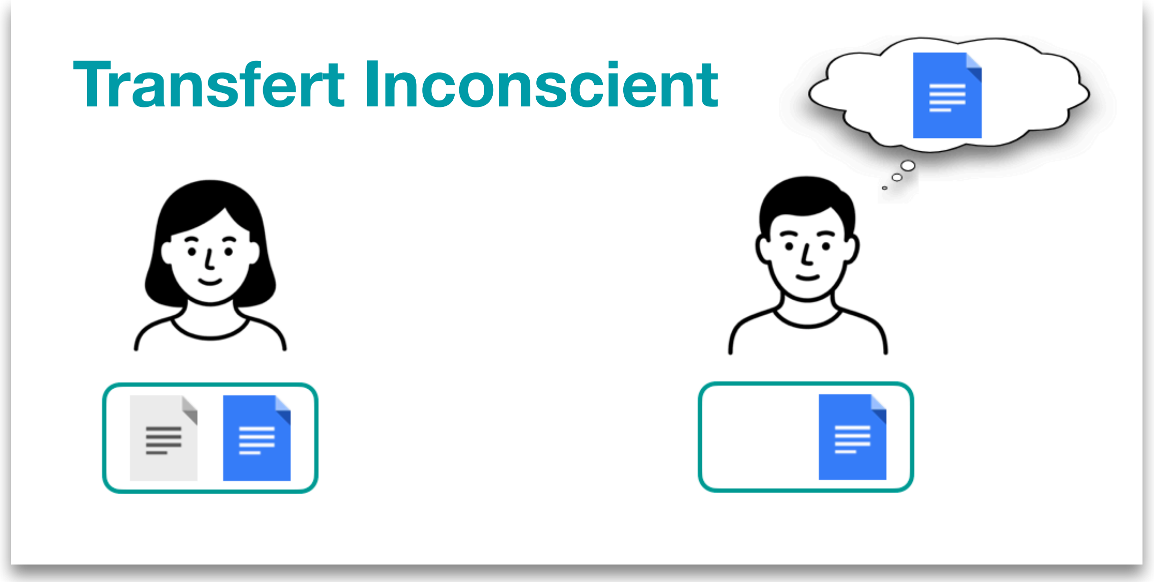


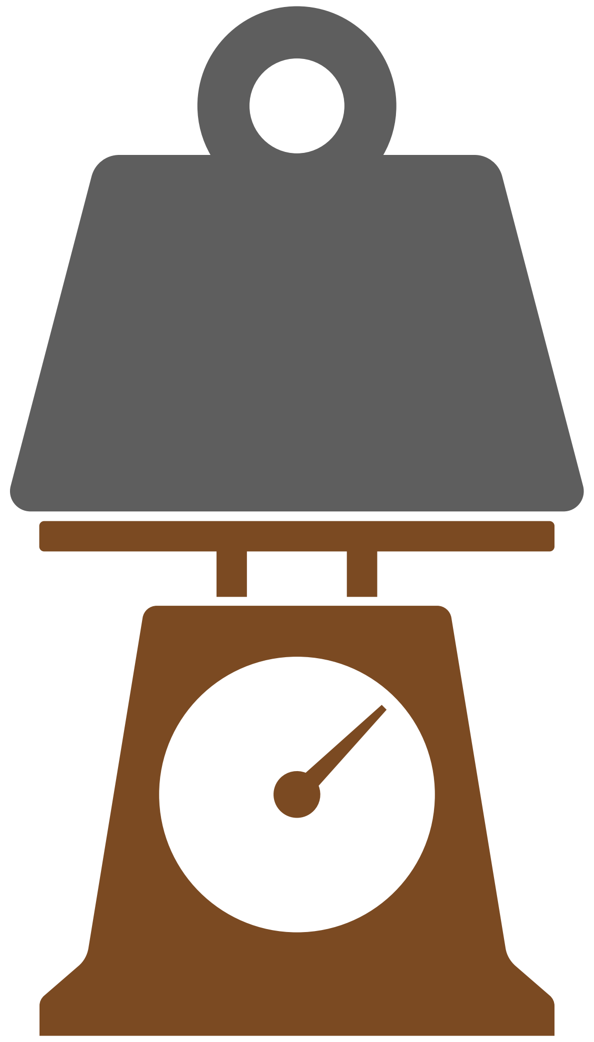
AAACGTACCTGACAAT

ACACGTACCTGACAAT

ACACGT_CCTGACAAT

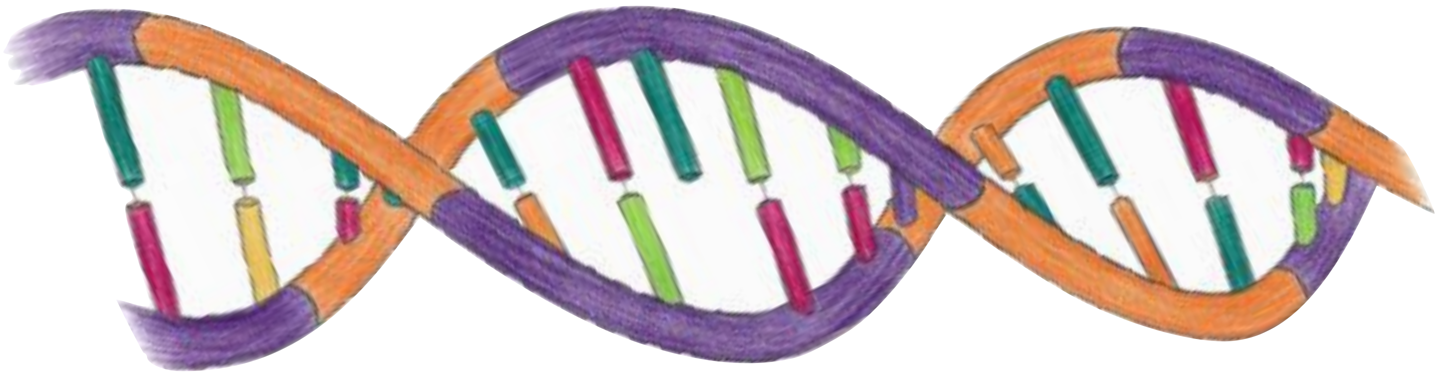




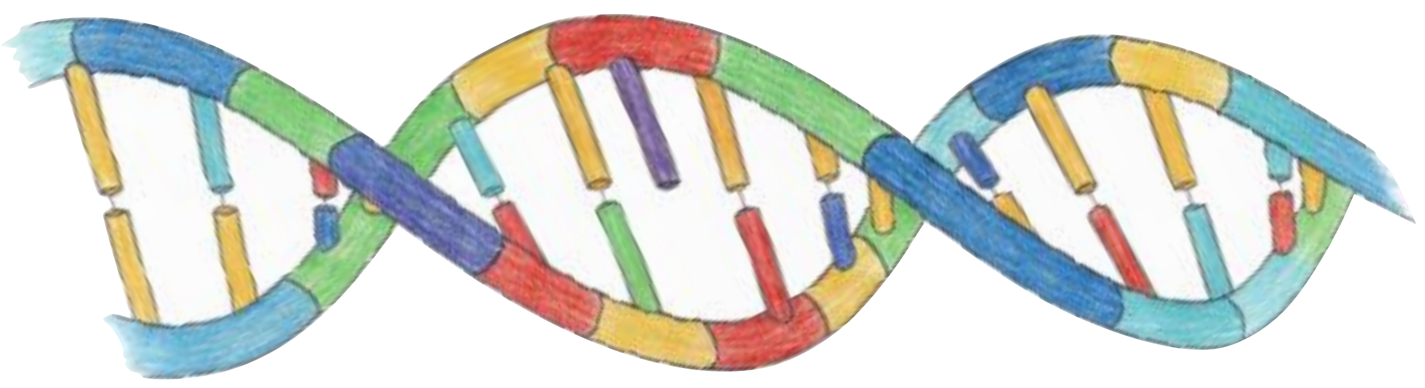


Exemple : distance d'édition

TACGCGTCTTGAGCT



Calcul sécurisé via le protocole GMW

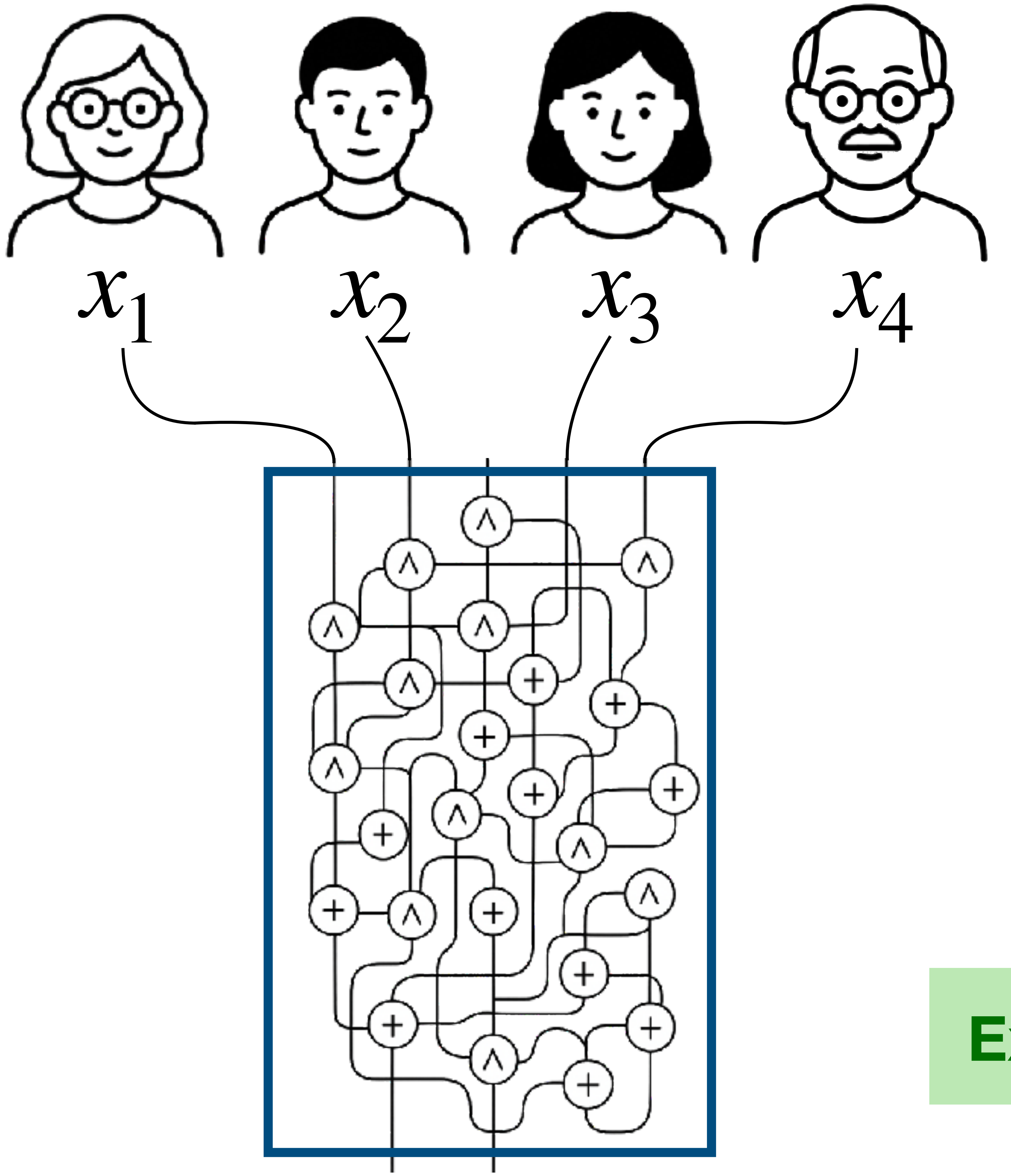


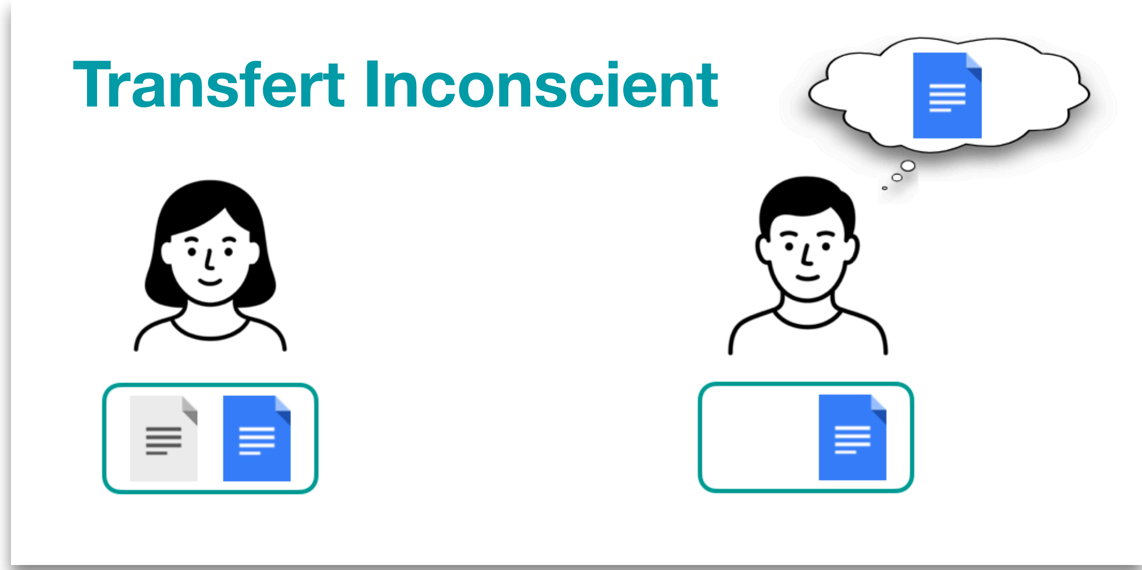
AAACGTACCTGACAAT

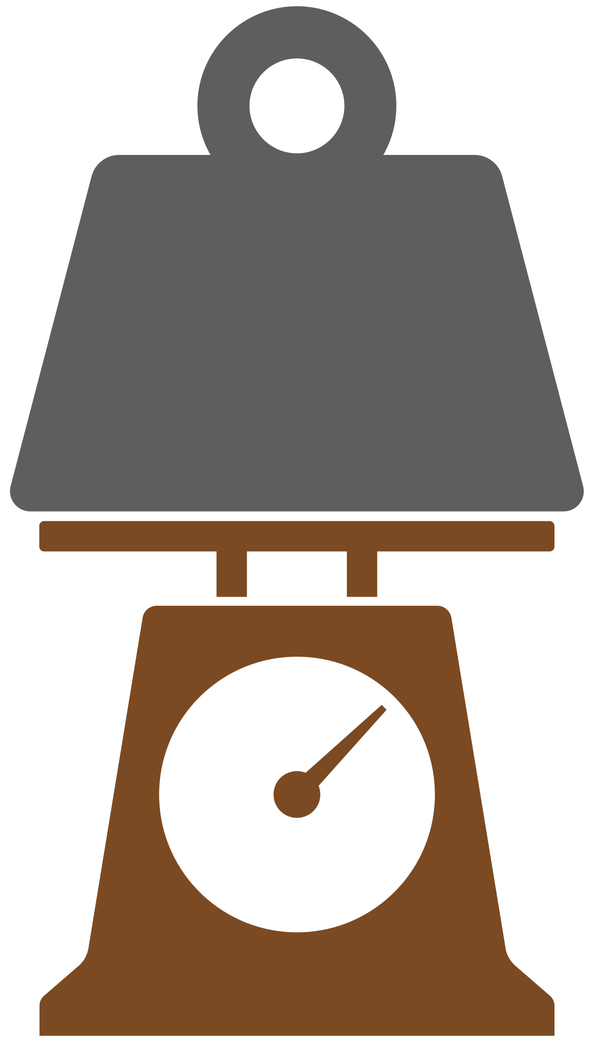
ACACGTACCTGACAAT

ACACGT_CCTGACAAT

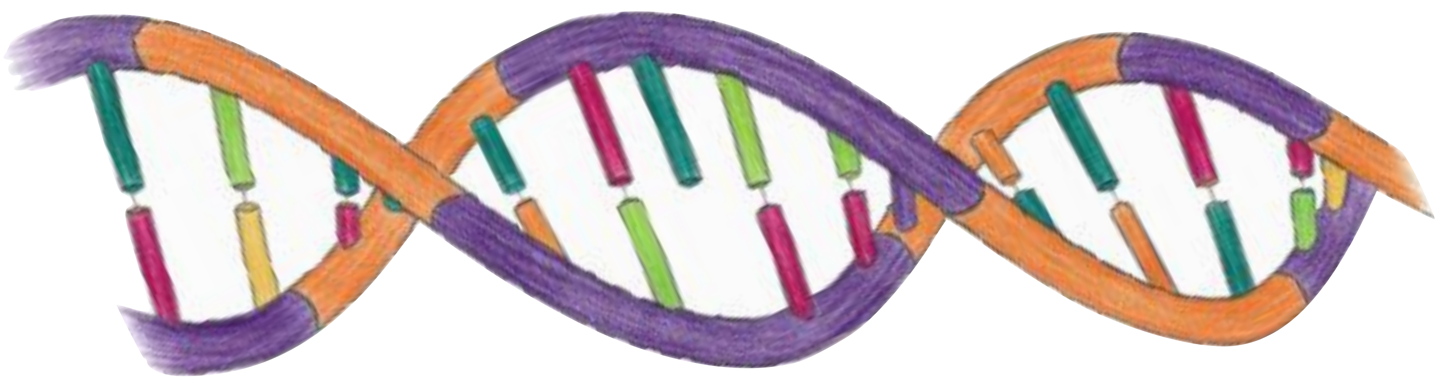
ACACGTCTTGACAAT





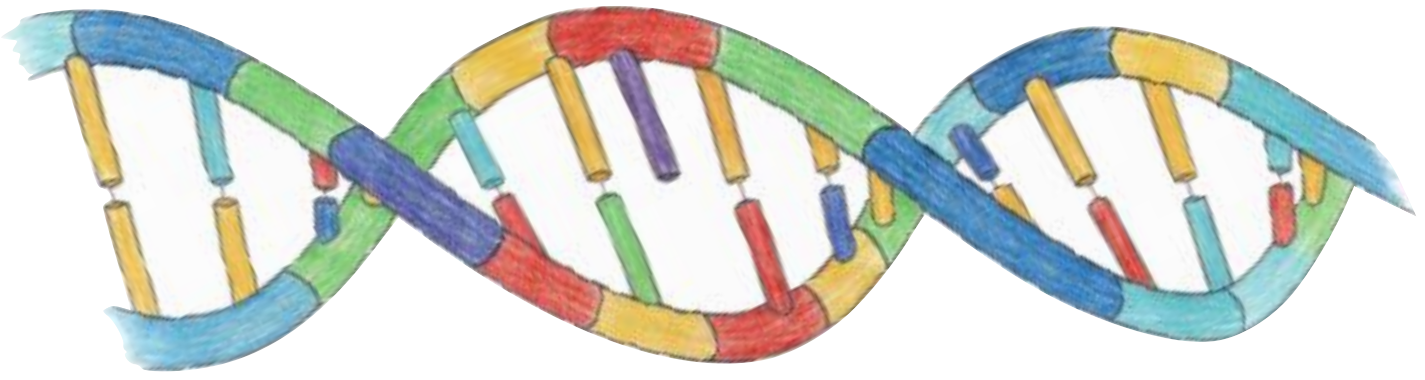


TACGCGTCTTGAGCT



Exemple : distance d'édition

Calcul sécurisé via le protocole GMW



AAACGTACCTGACAAT

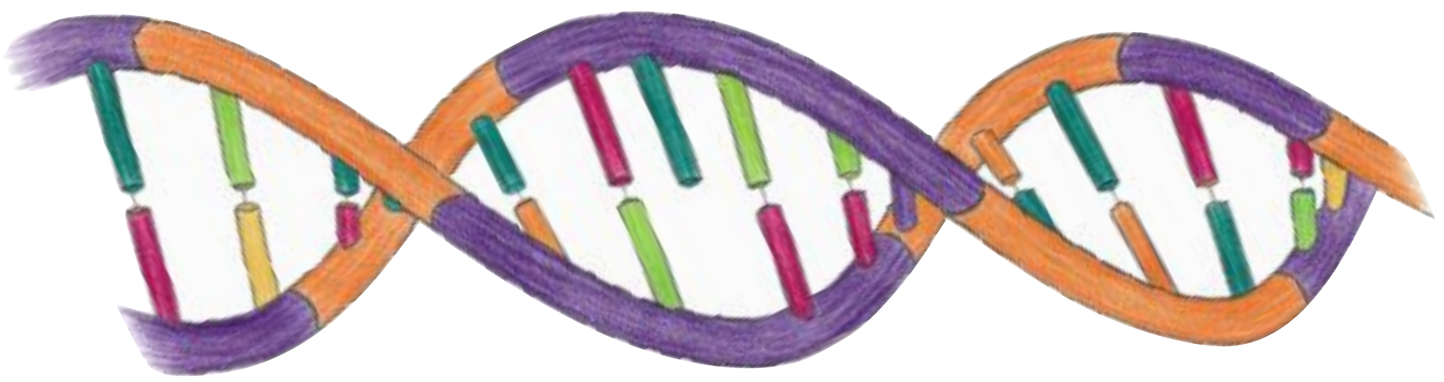
ACACGTACCTGACAAT

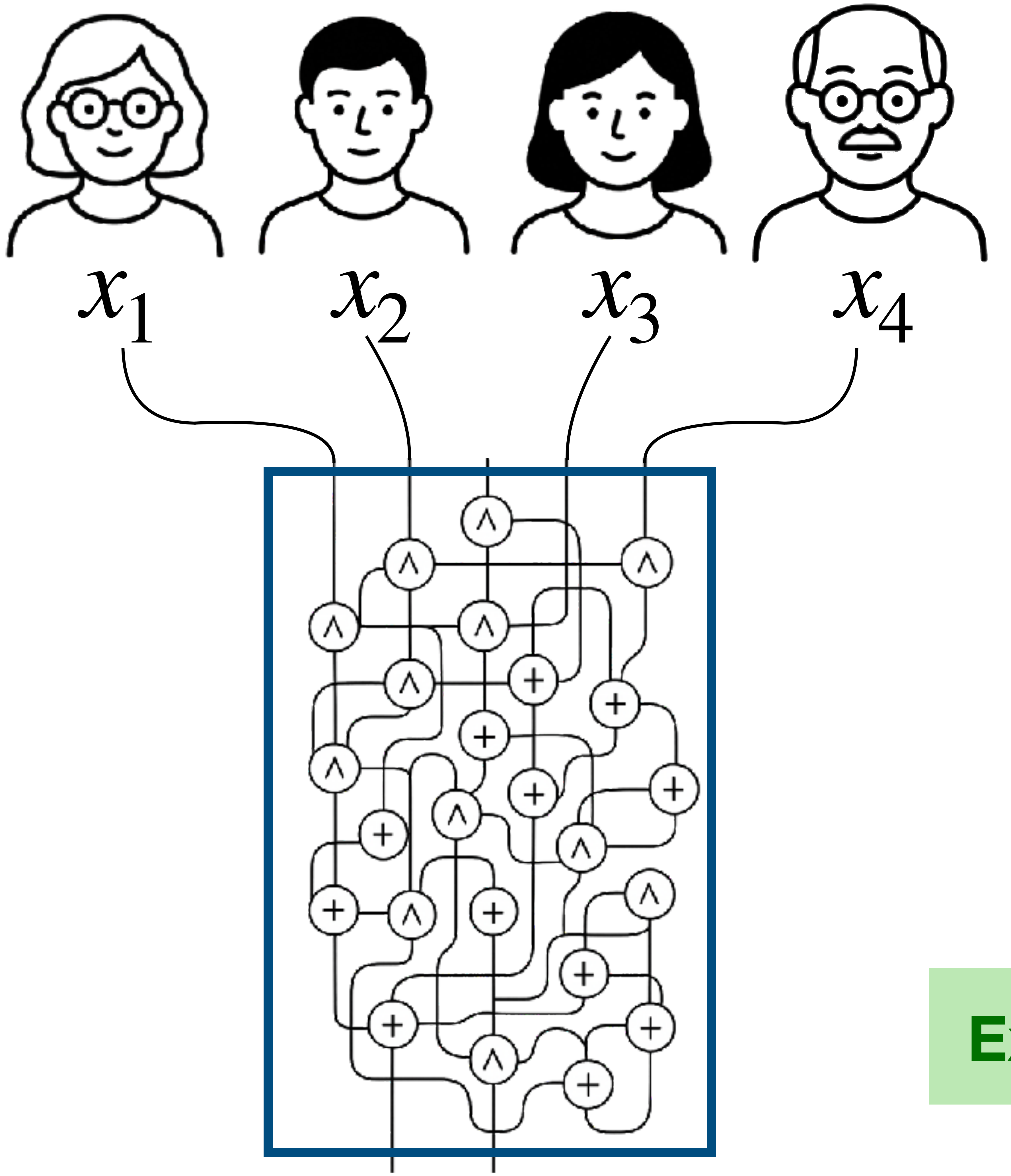
ACACGT_CCTGACAAT

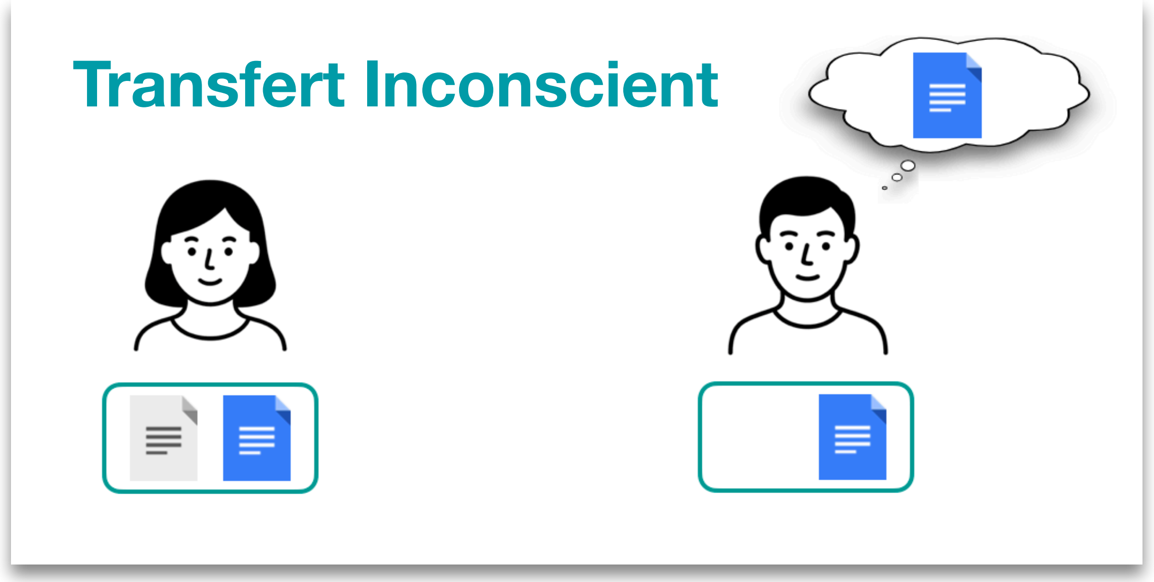
ACACGTCTTGACAAT

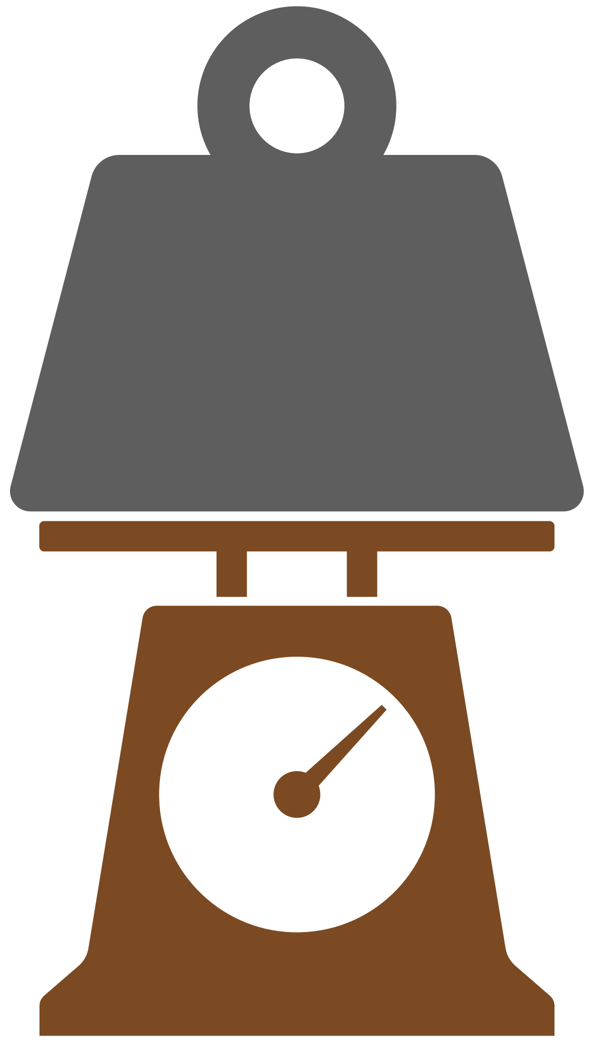
ACACGTCTTGAGCAAT

TACGCGTCTTGAGCT



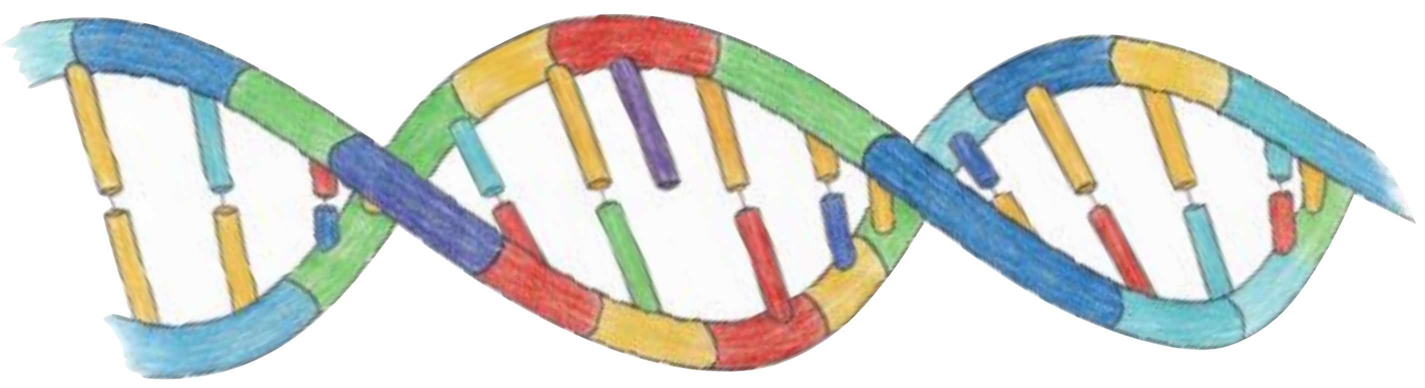






Exemple : distance d'édition

Calcul sécurisé via le protocole GMW



AAACGTACCTGACAAT

ACACGTACCTGACAAT

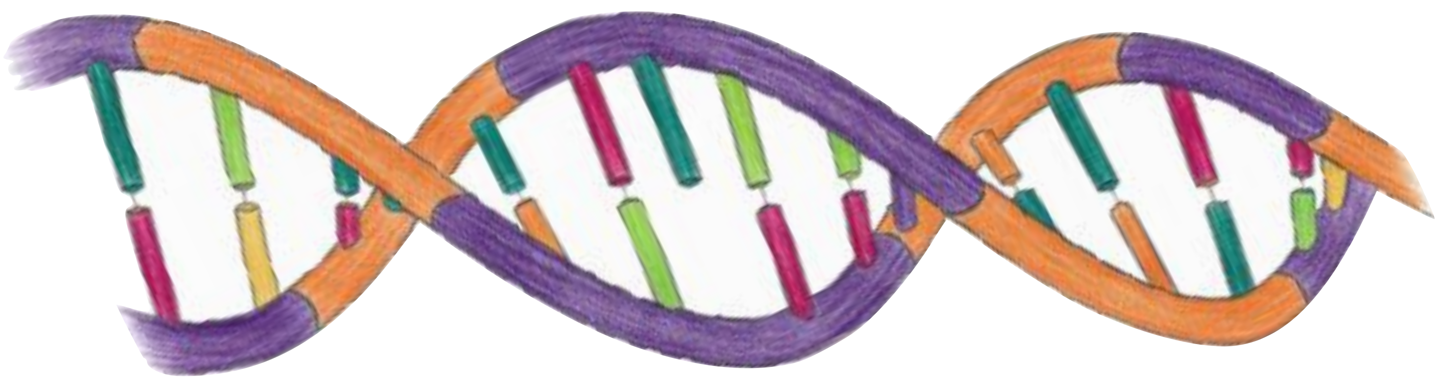
ACACGT_CCTGACAAT

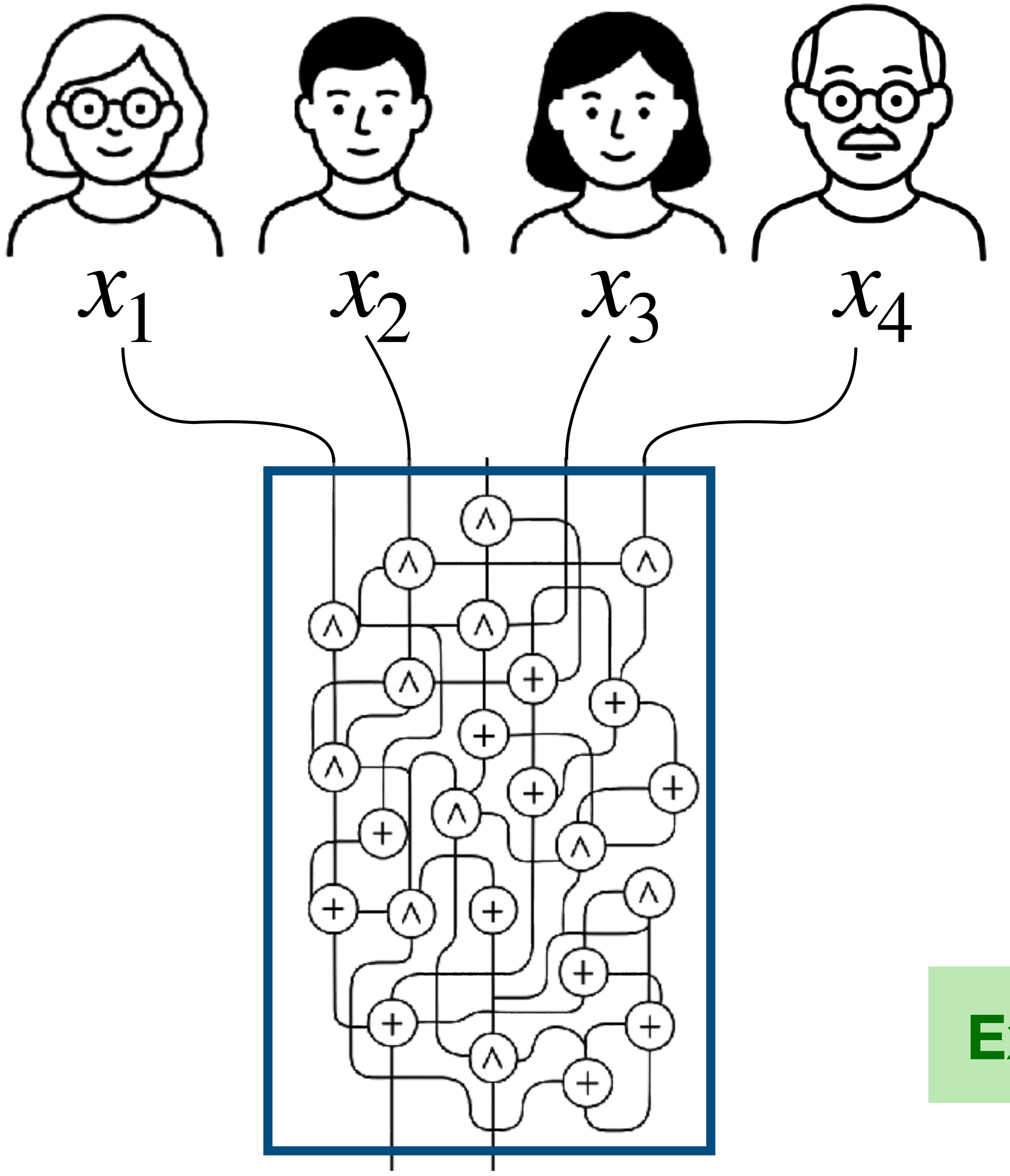
ACACGTCTTGACAAT

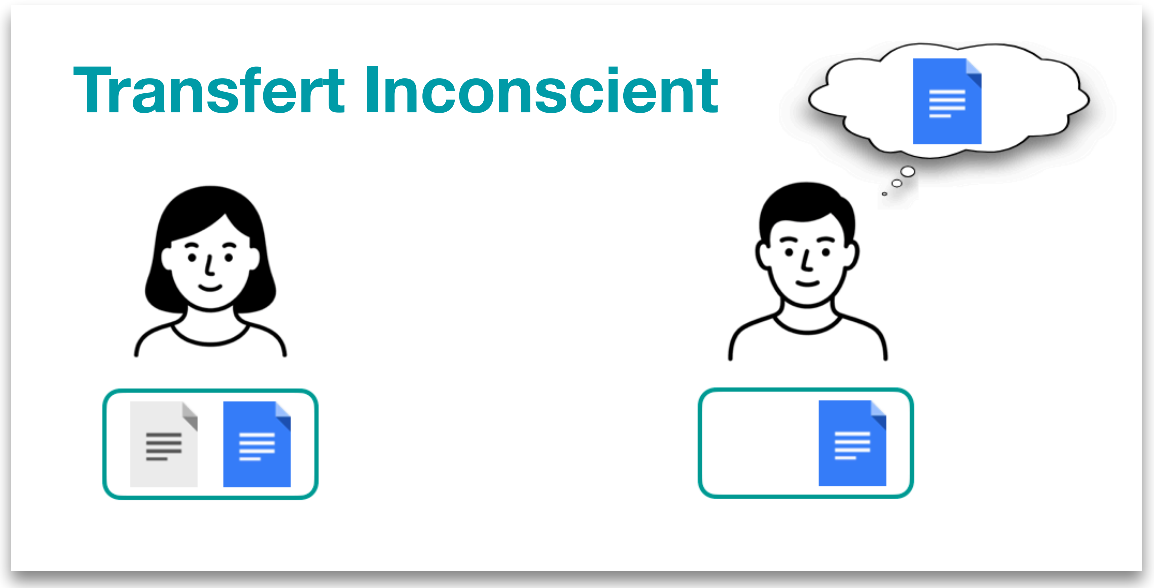
ACACGTCTTGAGCAAT

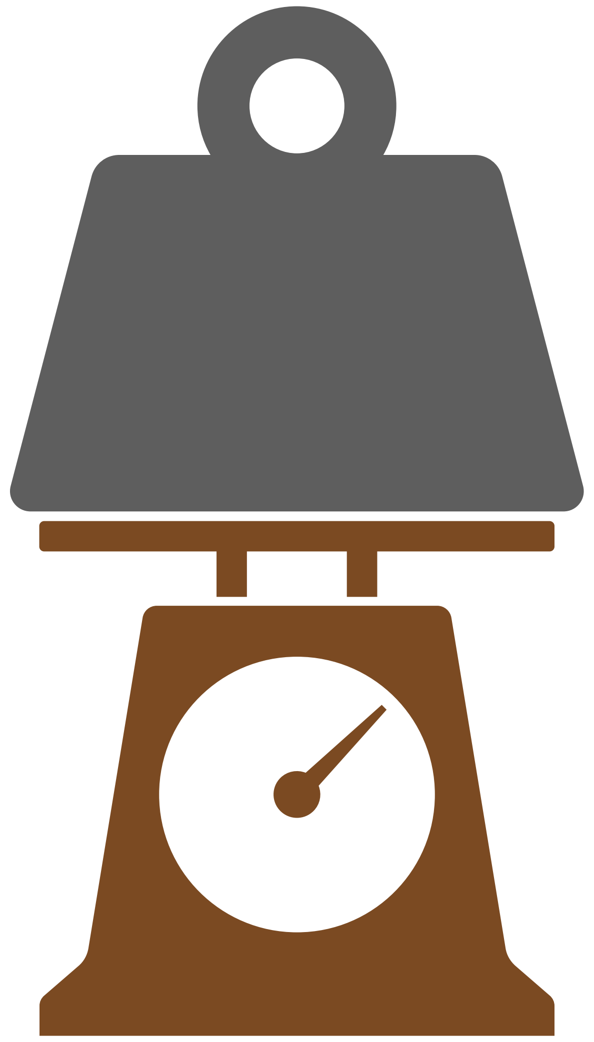
ACGCGTCTTGAGCAAT

TACGCGTCTTGAGCT



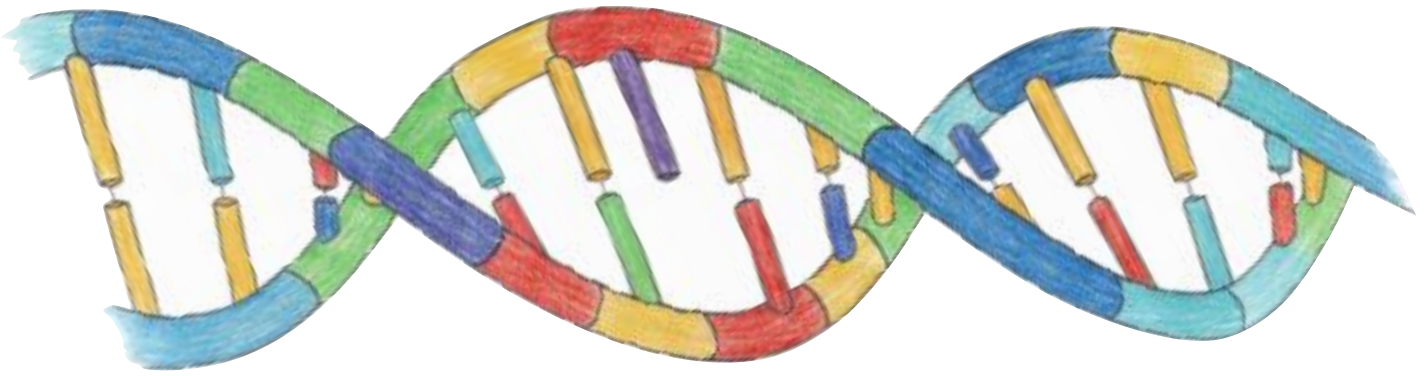






Exemple : distance d'édition

Calcul sécurisé via le protocole GMW



AAACGTACCTGACAAT

ACACGTACCTGACAAT

ACACGT_CCTGACAAT

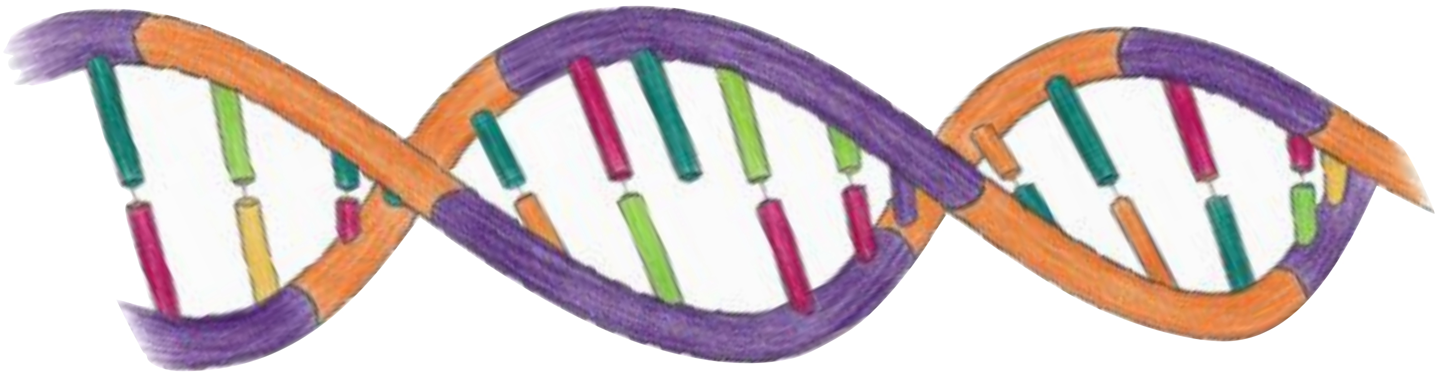
ACACGTCTTGACAAT

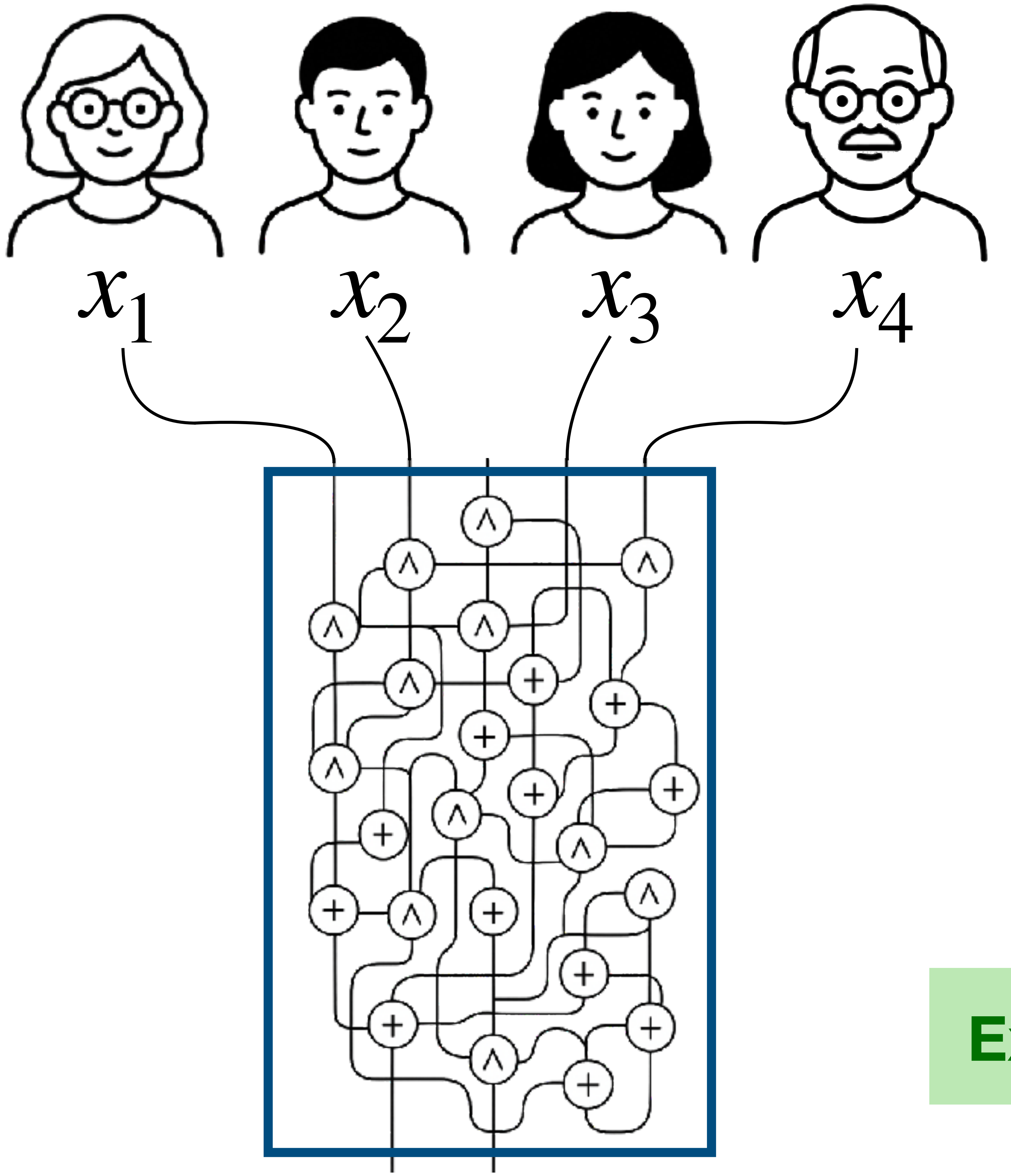
ACACGTCTTGAGCAAT

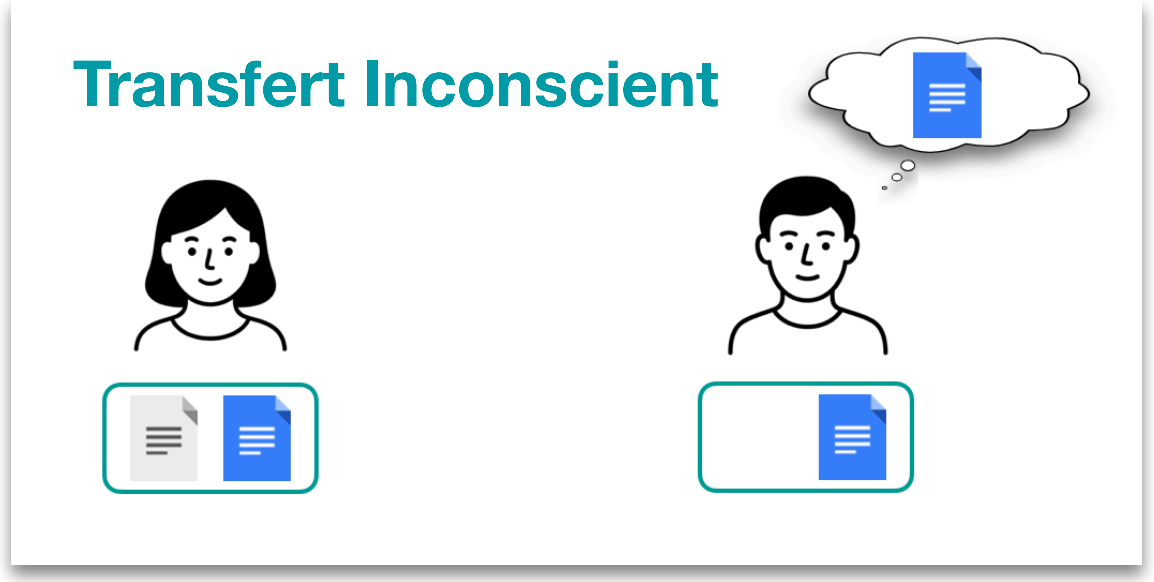
ACGCGTCTTGAGCAAT

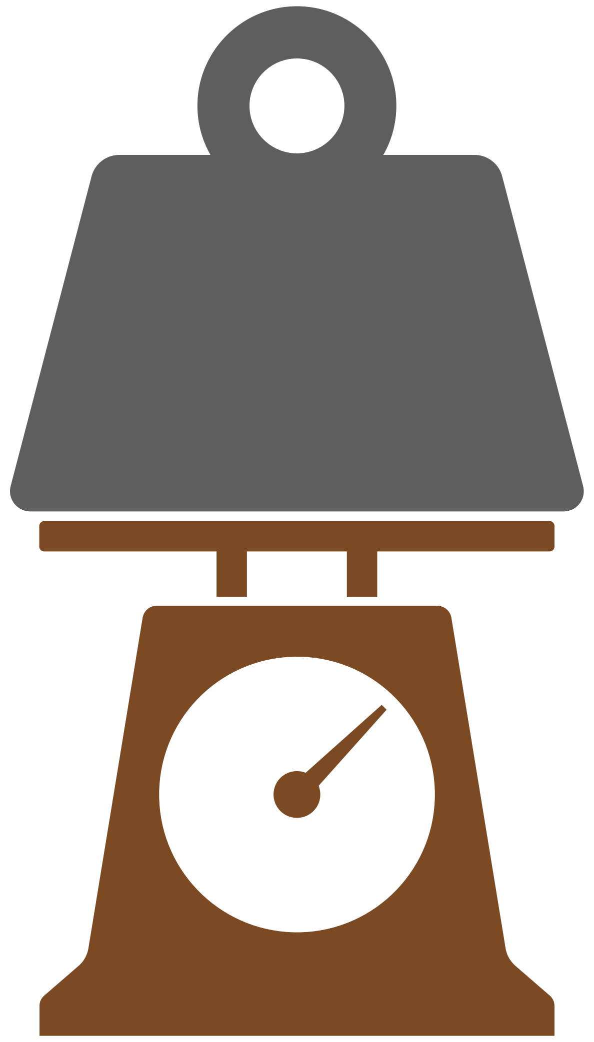
ACGCGTCTTGAGC_AT

TACGCGTCTTGAGCT



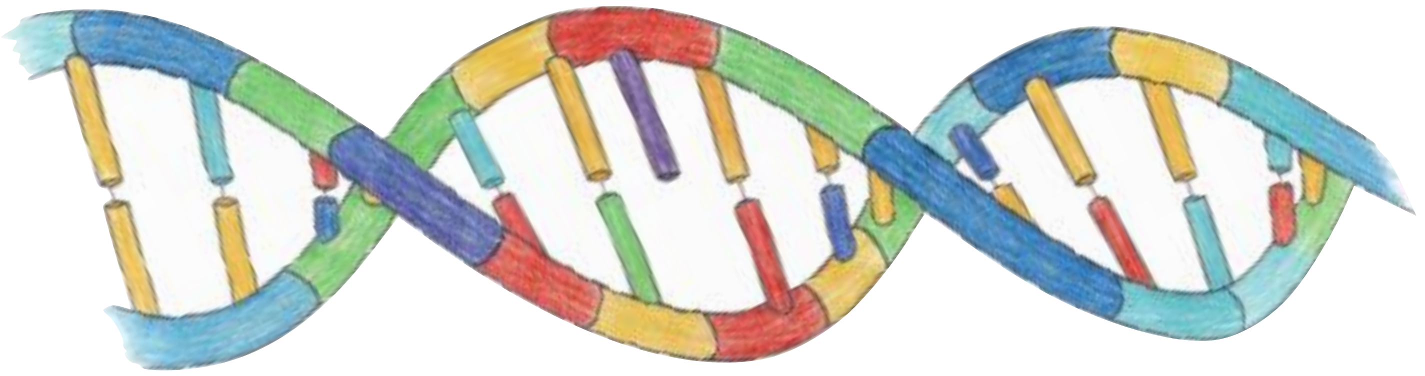




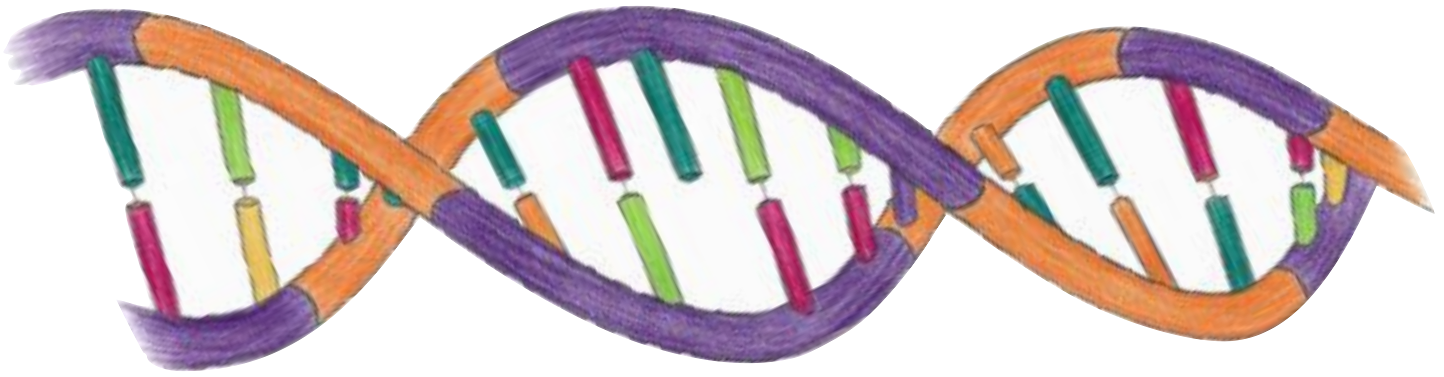


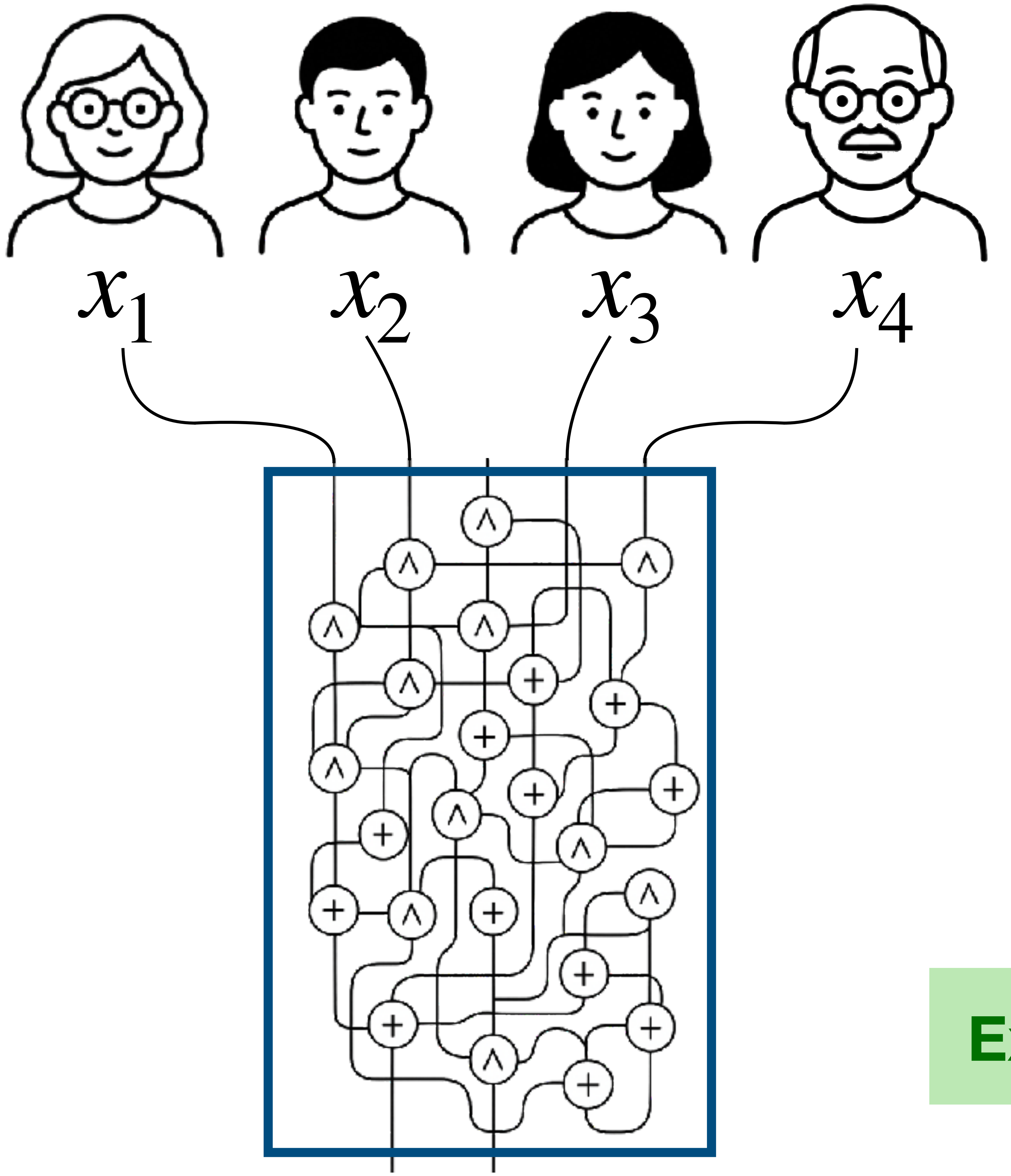
Exemple : distance d'édition

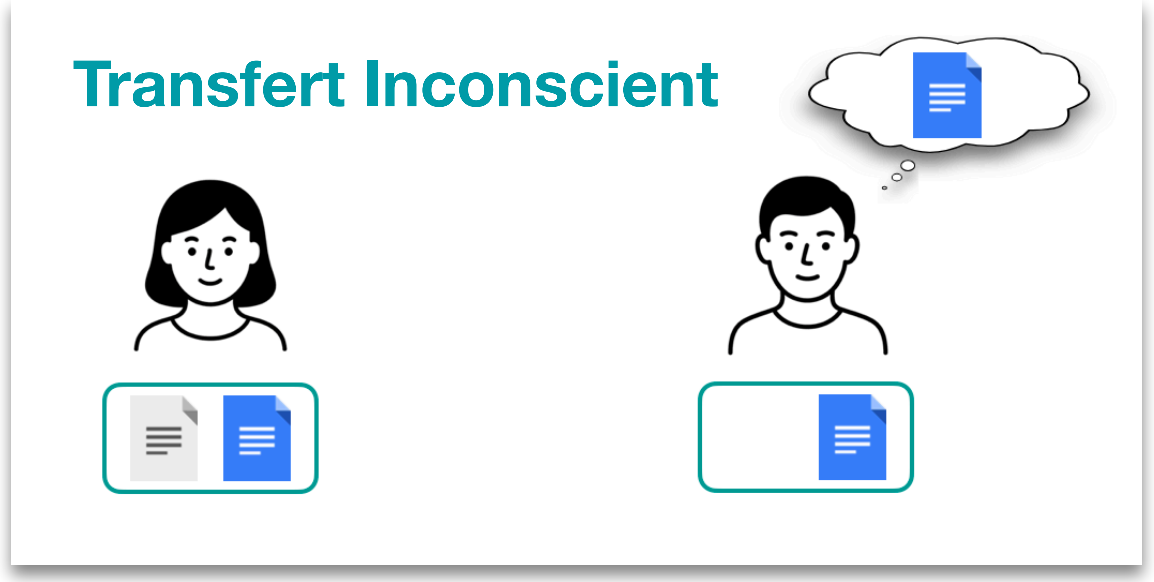
Calcul sécurisé via le protocole GMW

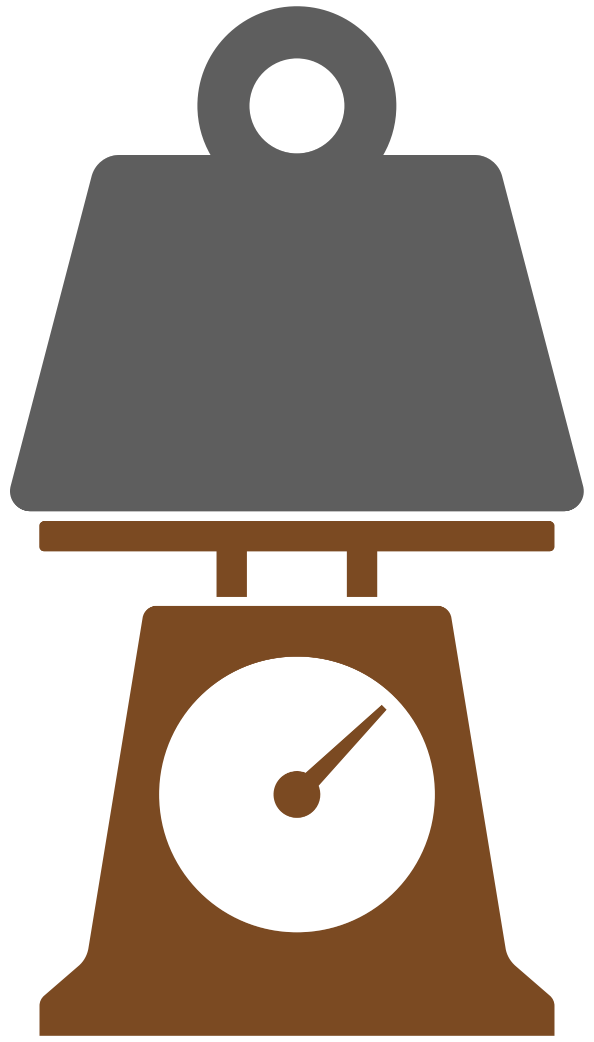


AAACGTACCTGACAAT
ACACGTACCTGACAAT
ACACGT_CCTGACAAT
ACACGTCTTGACAAT
ACACGTCTTGAGCAAT
ACGCGTCTTGAGCAAT
ACGCGTCTTGAGC_AT
ACGCGTCTTGAGC_T
TACGCGTCTTGAGCT



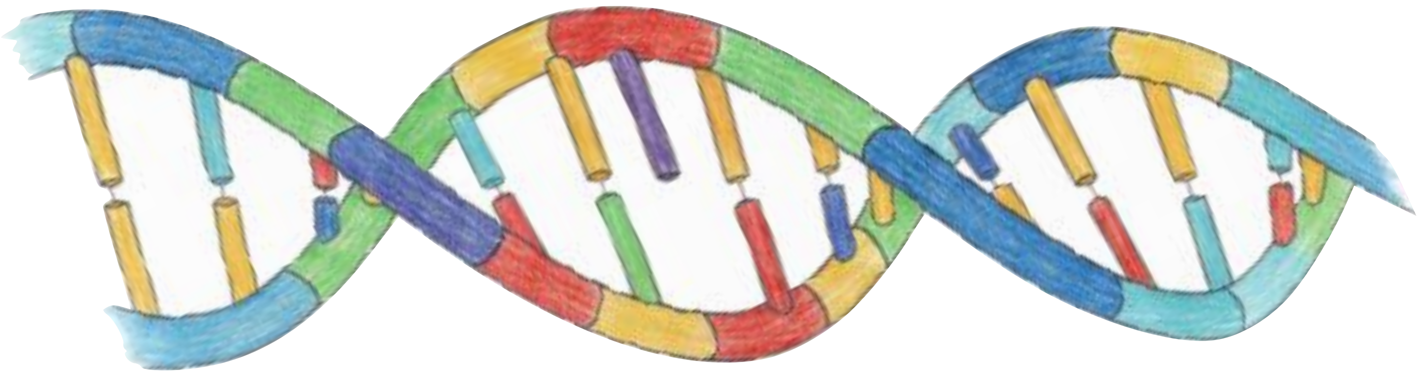






Exemple : distance d'édition

Calcul sécurisé via le protocole GMW



AAACGTACCTGACAAT

ACACGTACCTGACAAT

ACACGT_CCTGACAAT

ACACGTCTTGACAAT

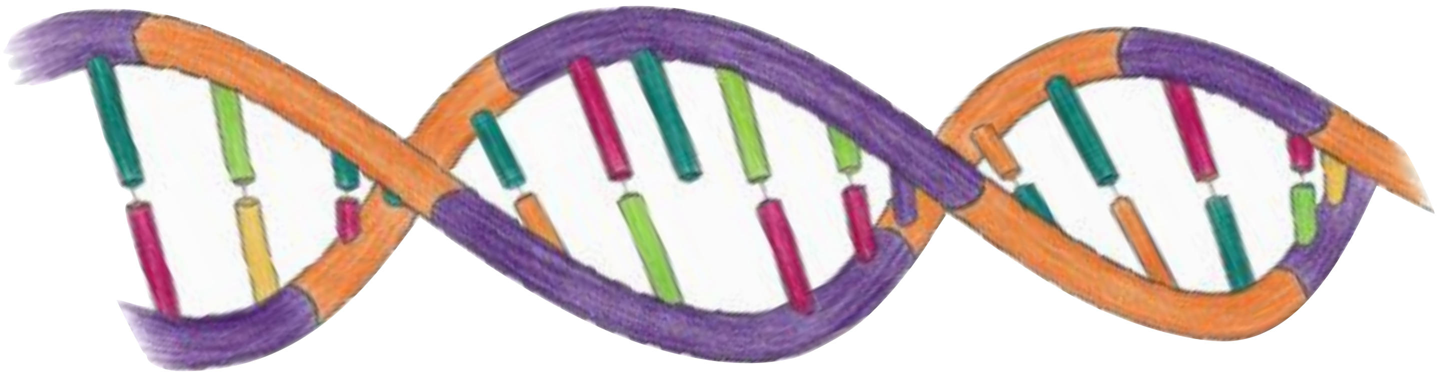
ACACGTCTTGAGCAAT

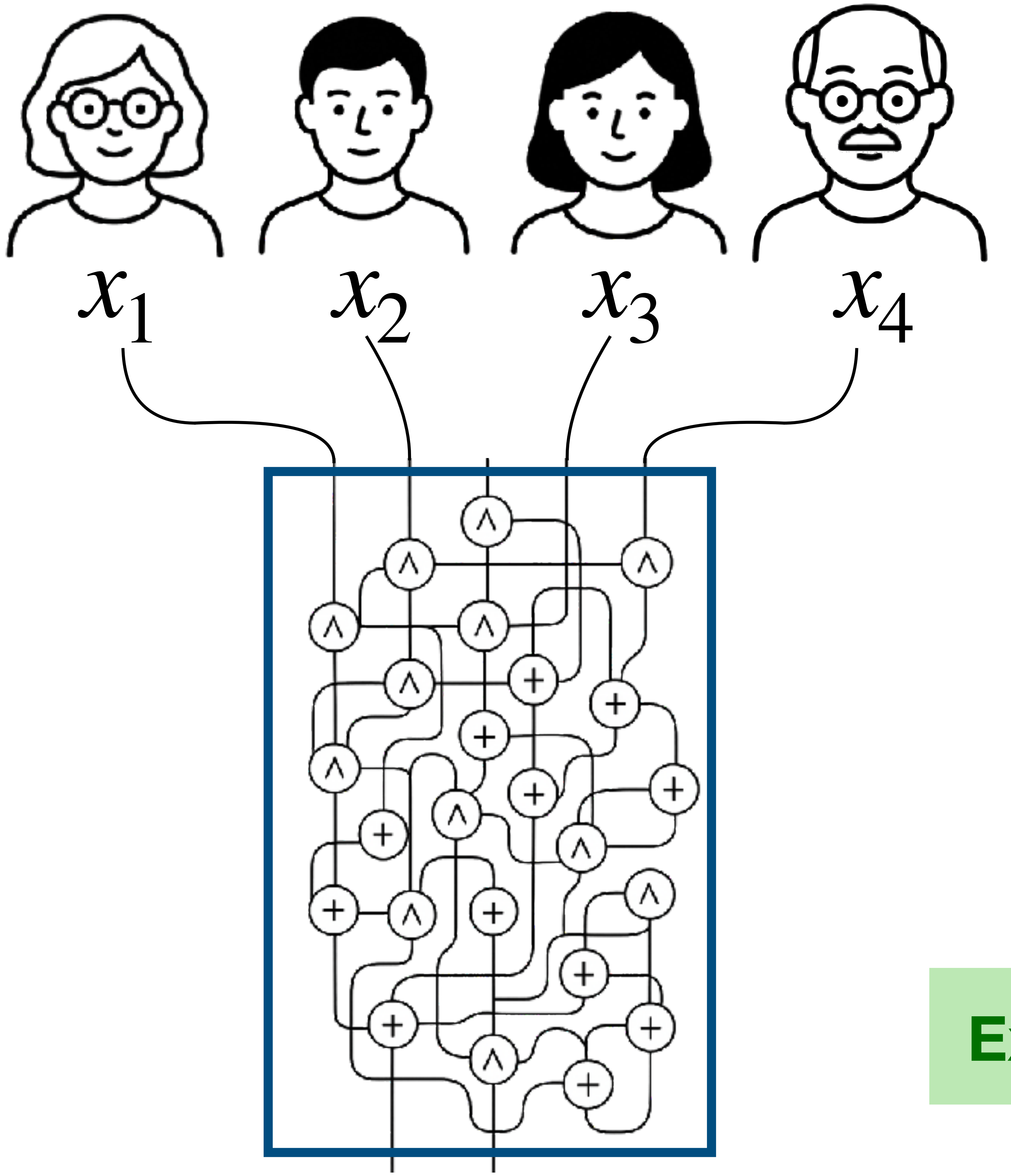
ACGCGTCTTGAGCAAT

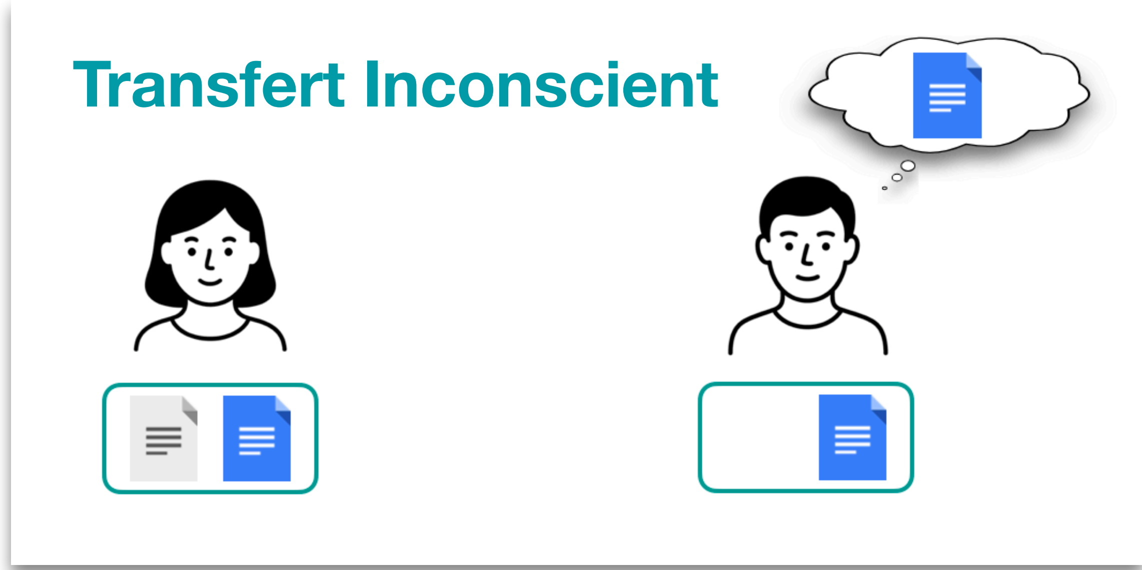
ACGCGTCTTGAGC_AT

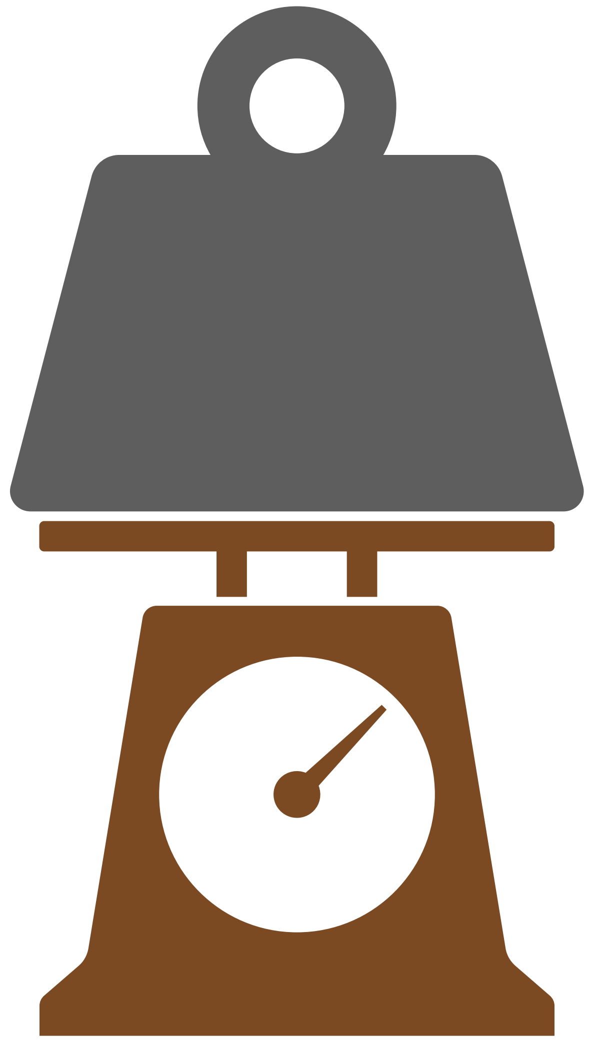
ACGCGTCTTGAGC_T

TACGCGTCTTGAGCT



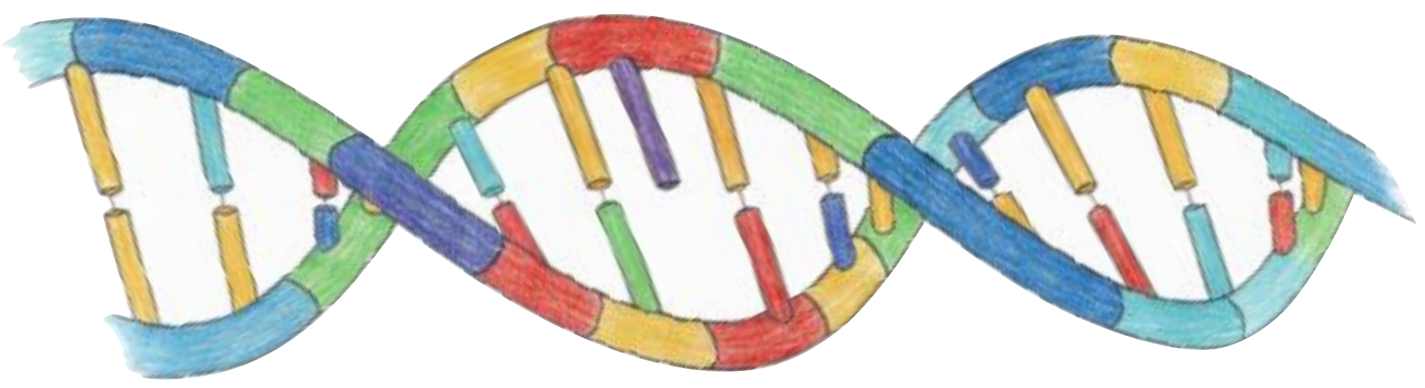




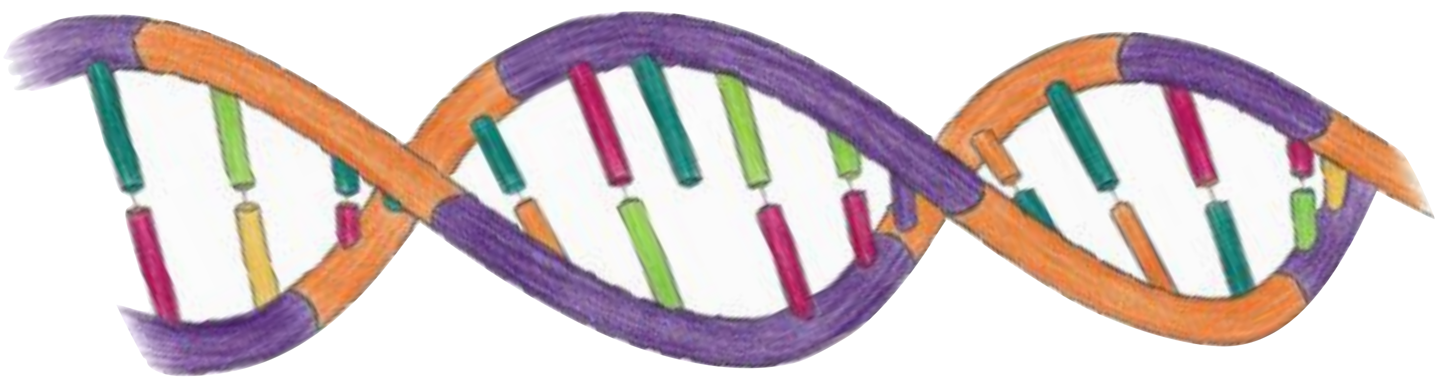


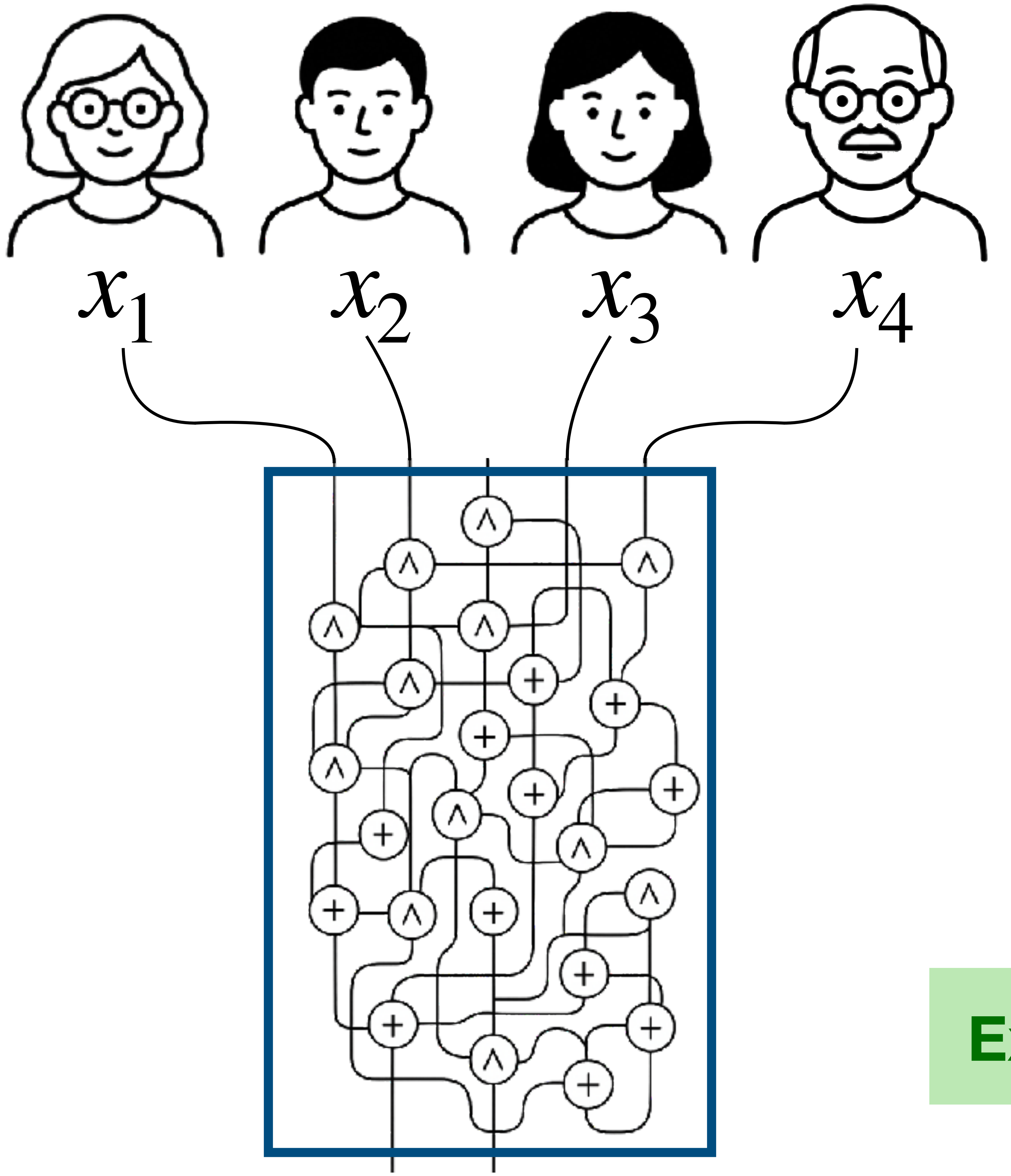
Exemple : distance d'édition

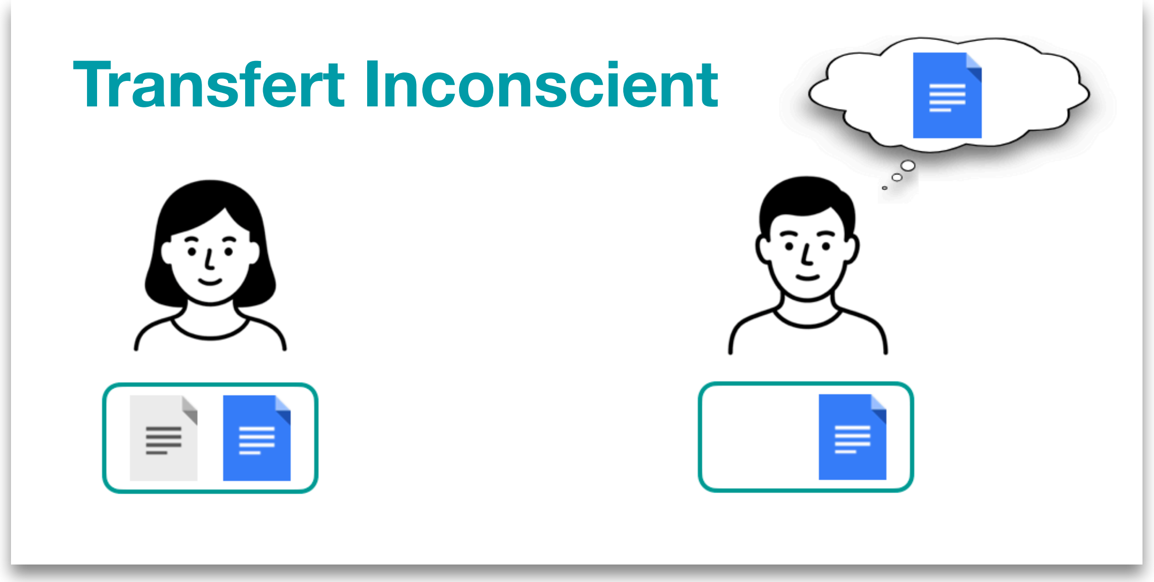
Calcul sécurisé via le protocole GMW

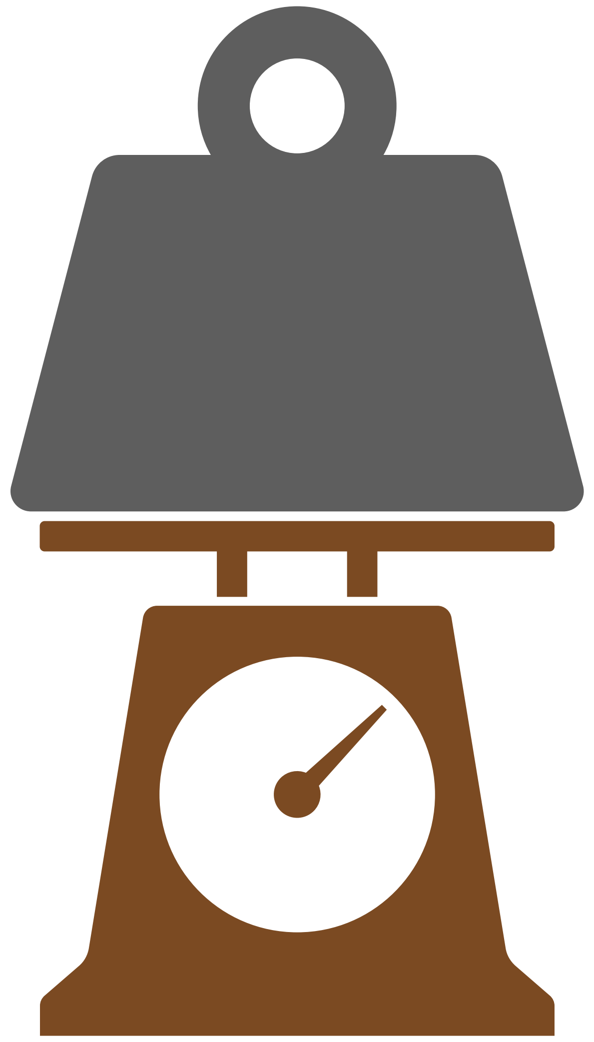


AAACGTACCTGACAAT
ACACGTACCTGACAAT
ACACGT_CCTGACAAT
ACACGTCTTGACAAT
8 ACACGTCTTGAGCAAT
ACGCGTCTTGAGCAAT
ACGCGTCTTGAGC_AT
ACGCGTCTTGAGC_T
TACGCGTCTTGAGCT





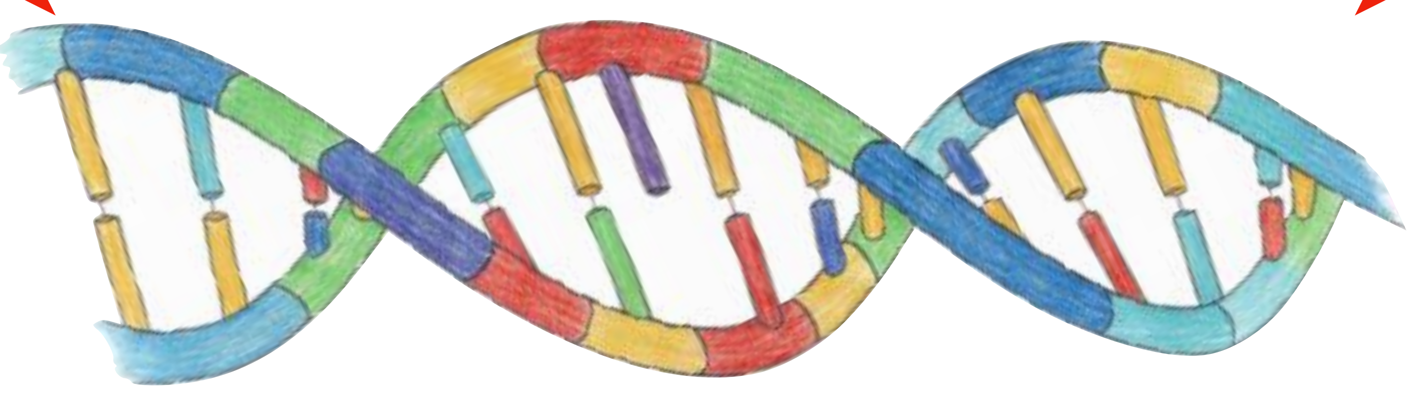




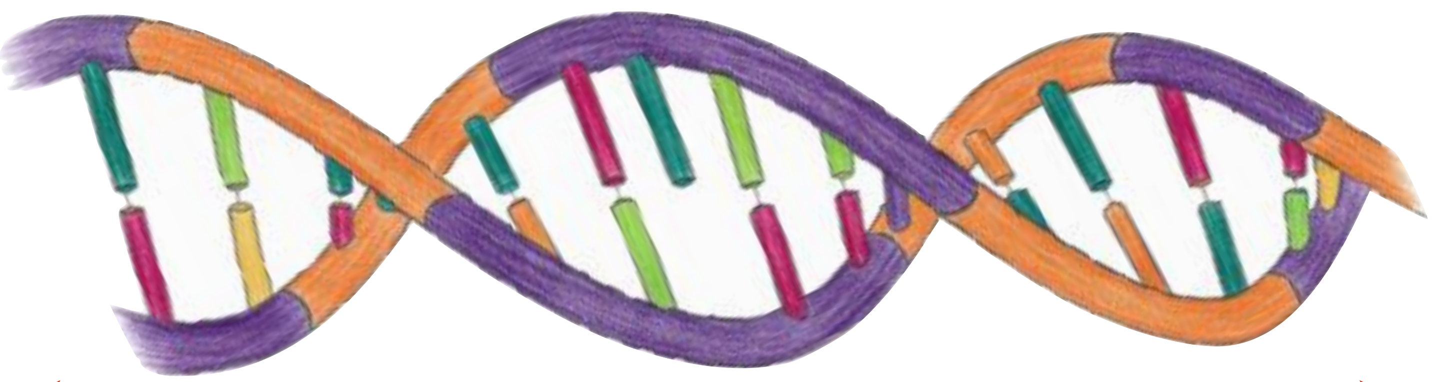
Exemple : distance d'édition

Calcul sécurisé via le protocole GMW

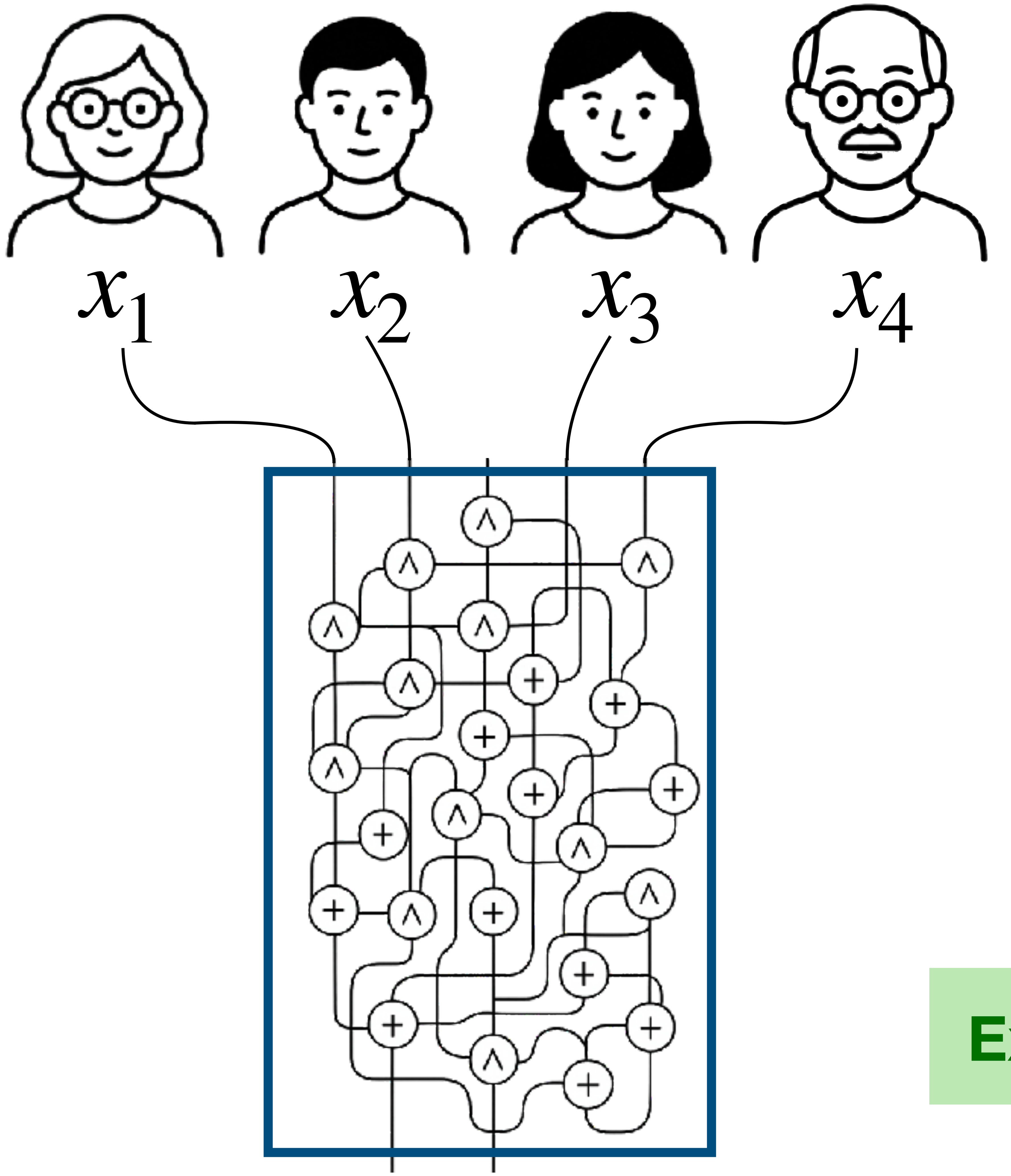
512 octets

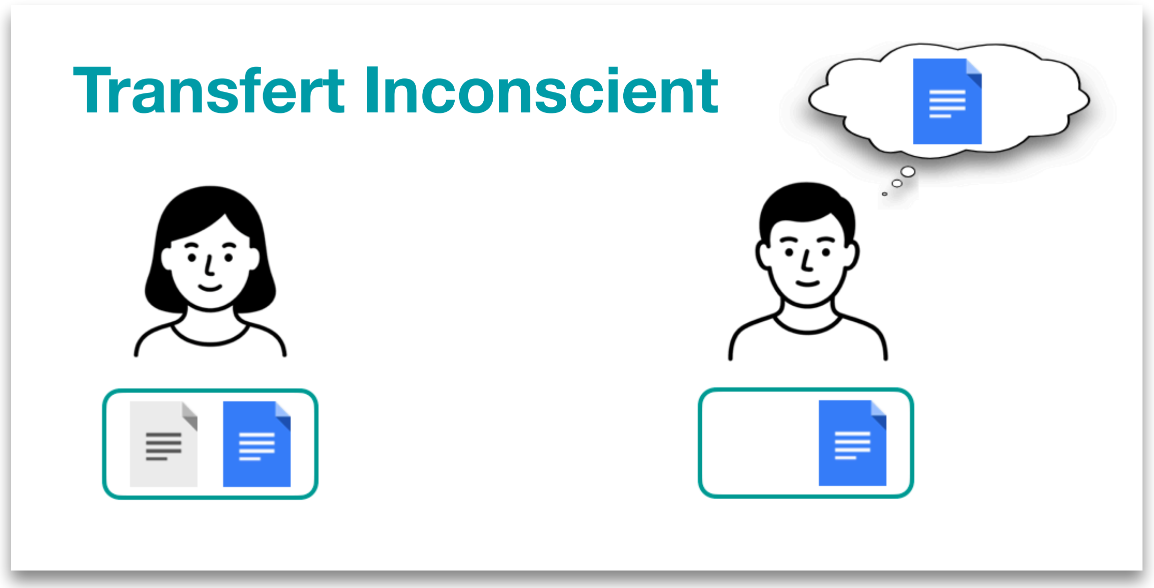


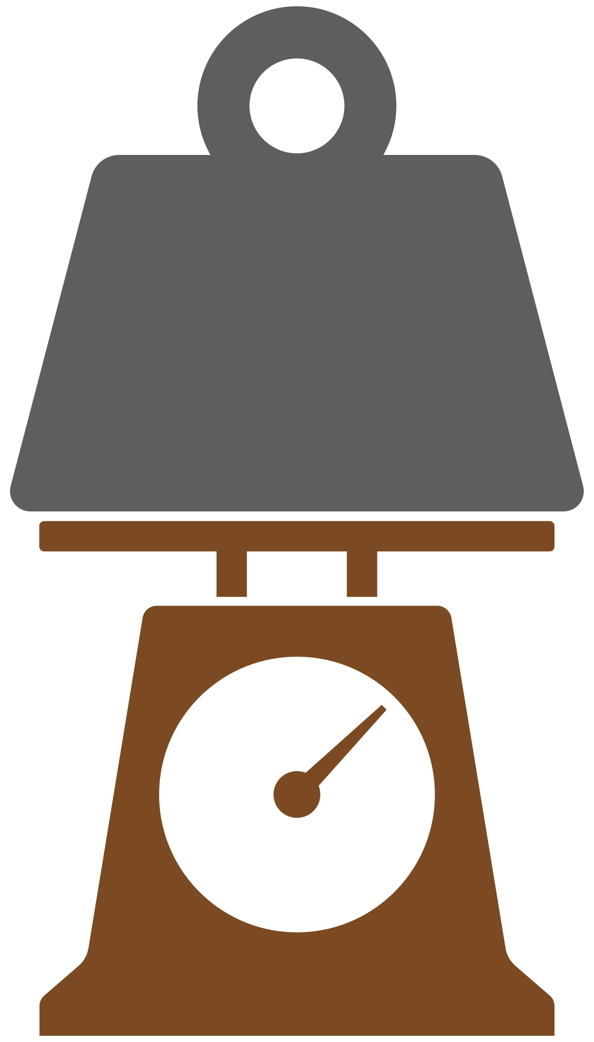
AAACGTACCTGACAAT
ACACGTACCTGACAAT
ACACGT_CCTGACAAT
ACACGTCTTGACAAT
8 ACACGTCTTGAGCAAT
ACGCGTCTTGAGCAAT
ACGCGTCTTGAGC_AT
ACGCGTCTTGAGC_T
TACGCGTCTTGAGCT



512 octets



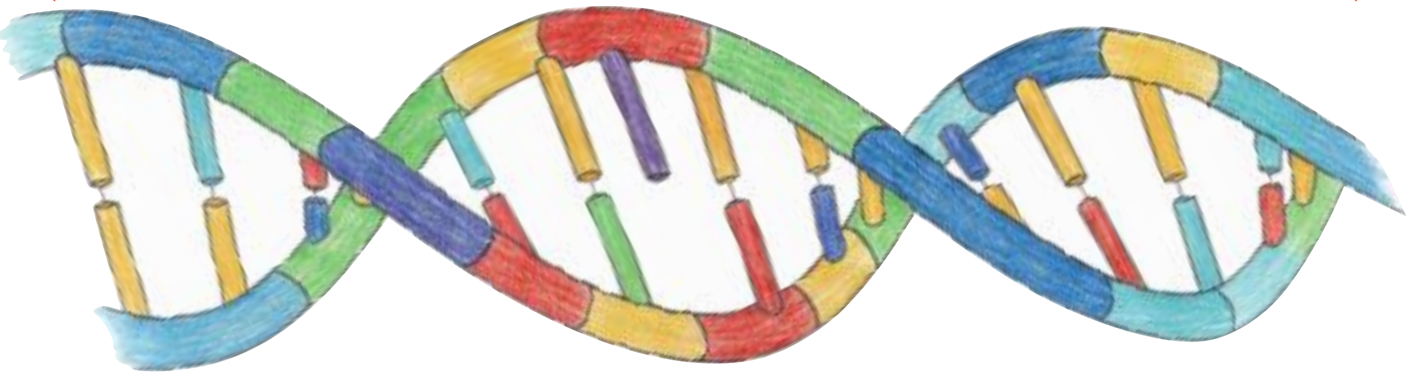




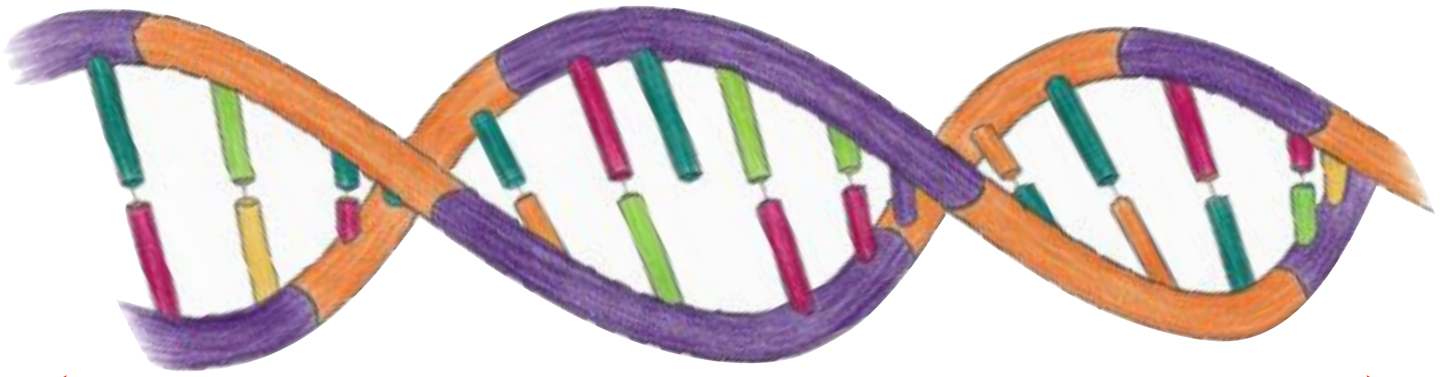
Exemple : distance d'édition

Calcul sécurisé via le protocole GMW

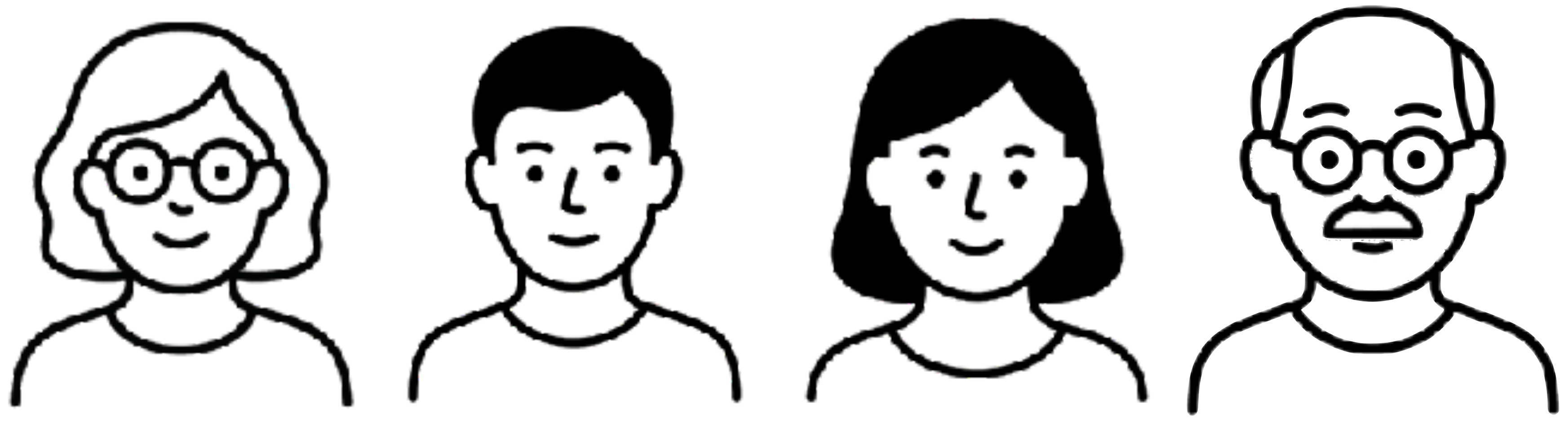
512 octets



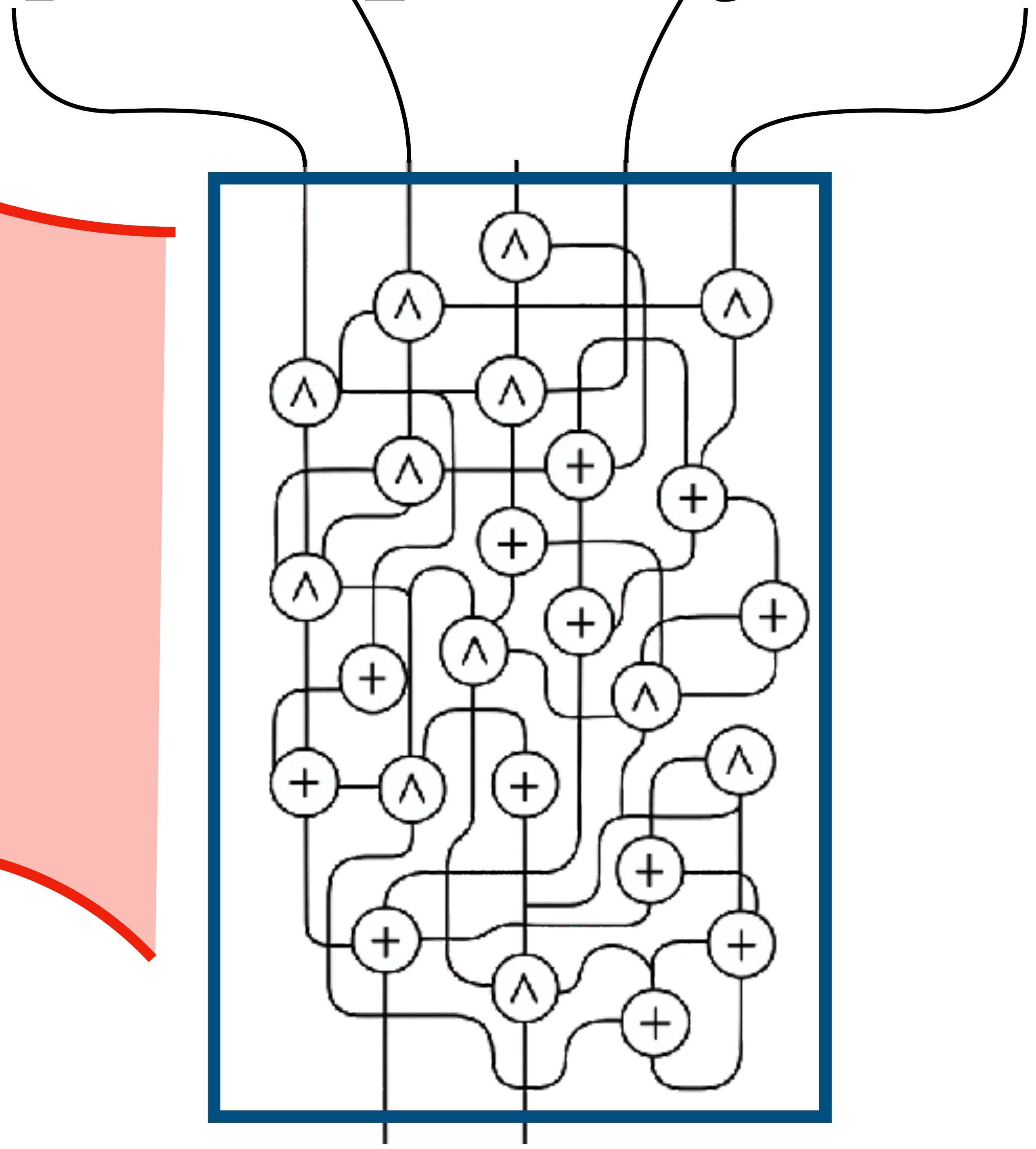
AAACGTACCTGACAAT
ACACGTACCTGACAAT
ACACGT_CCTGACAAT
ACACGTCTTGACAAT
8 ACACGTCTTGAGCAAT
ACGCGTCTTGAGCAAT
ACGCGTCTTGAGC_AT
ACGCGTCTTGAGC_T
TACGCGTCTTGAGCT



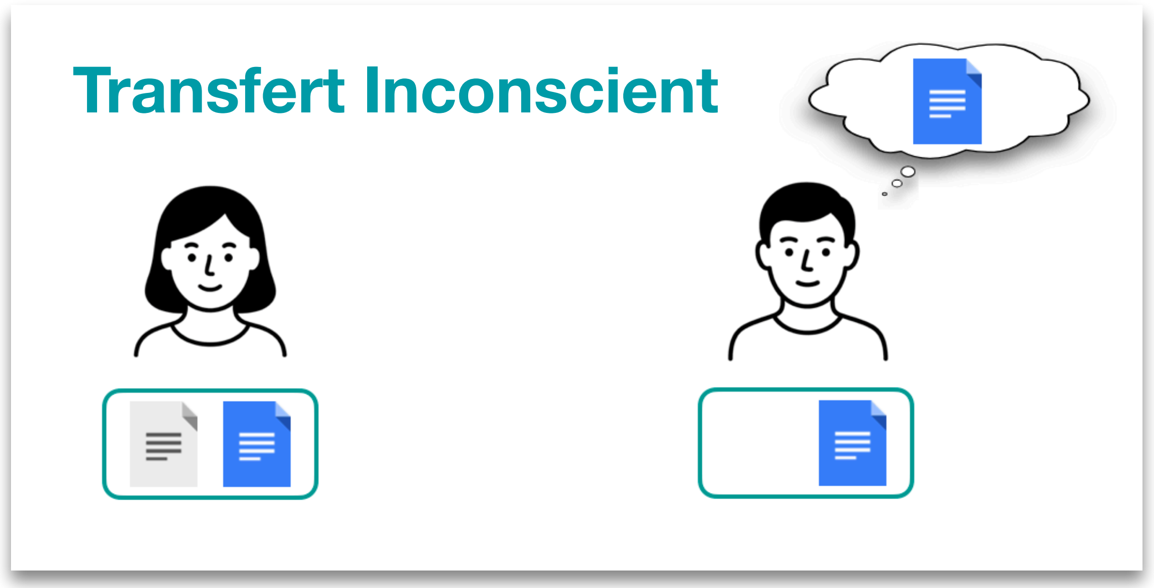
512 octets

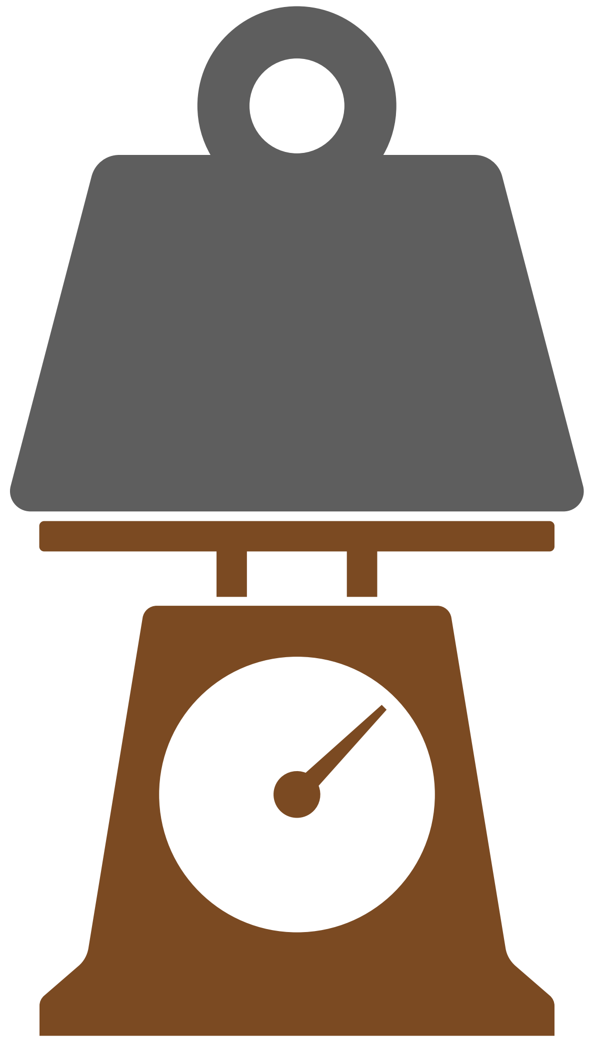


x_1 x_2 x_3 x_4



5,901,194,475 portes

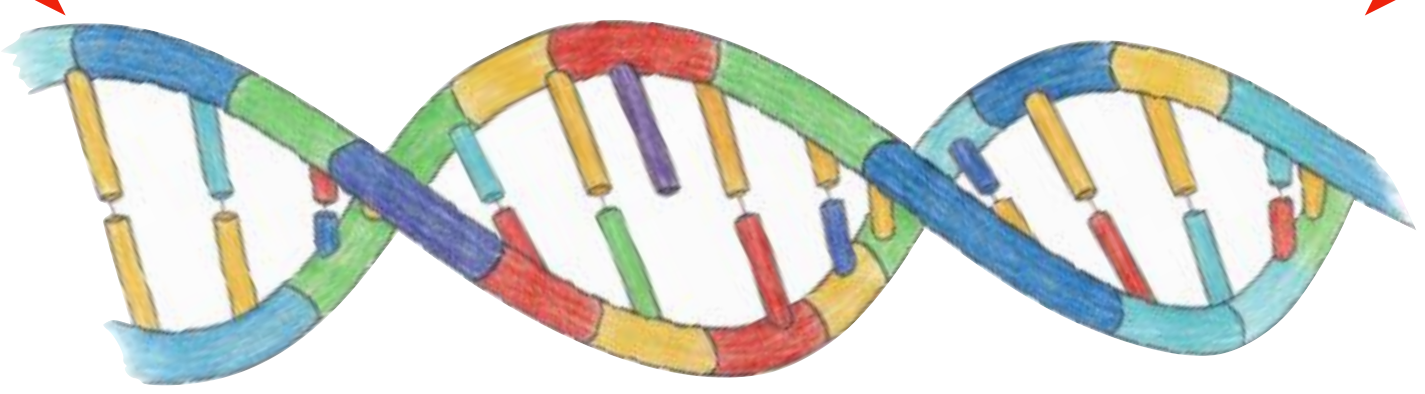




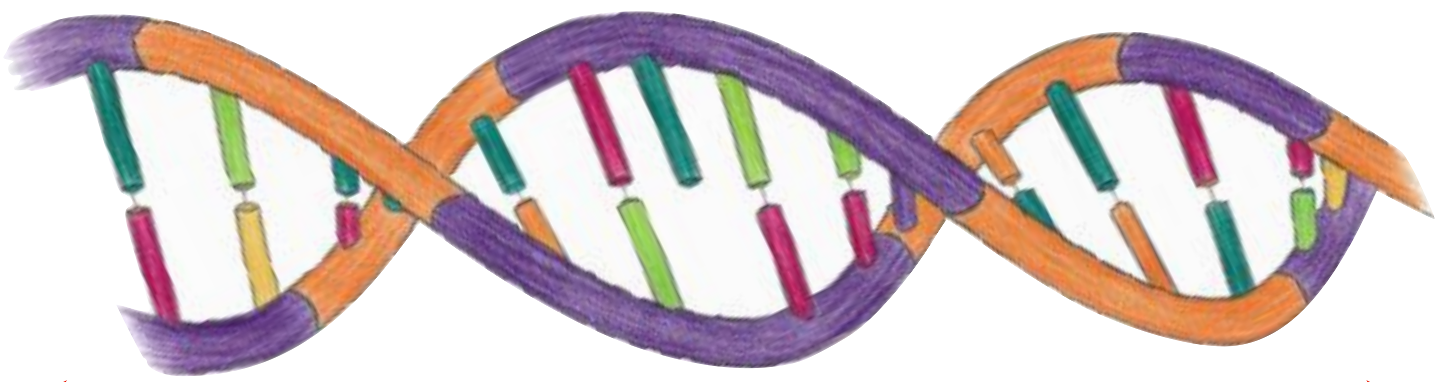
Exemple : distance d'édition

Calcul sécurisé via le protocole GMW

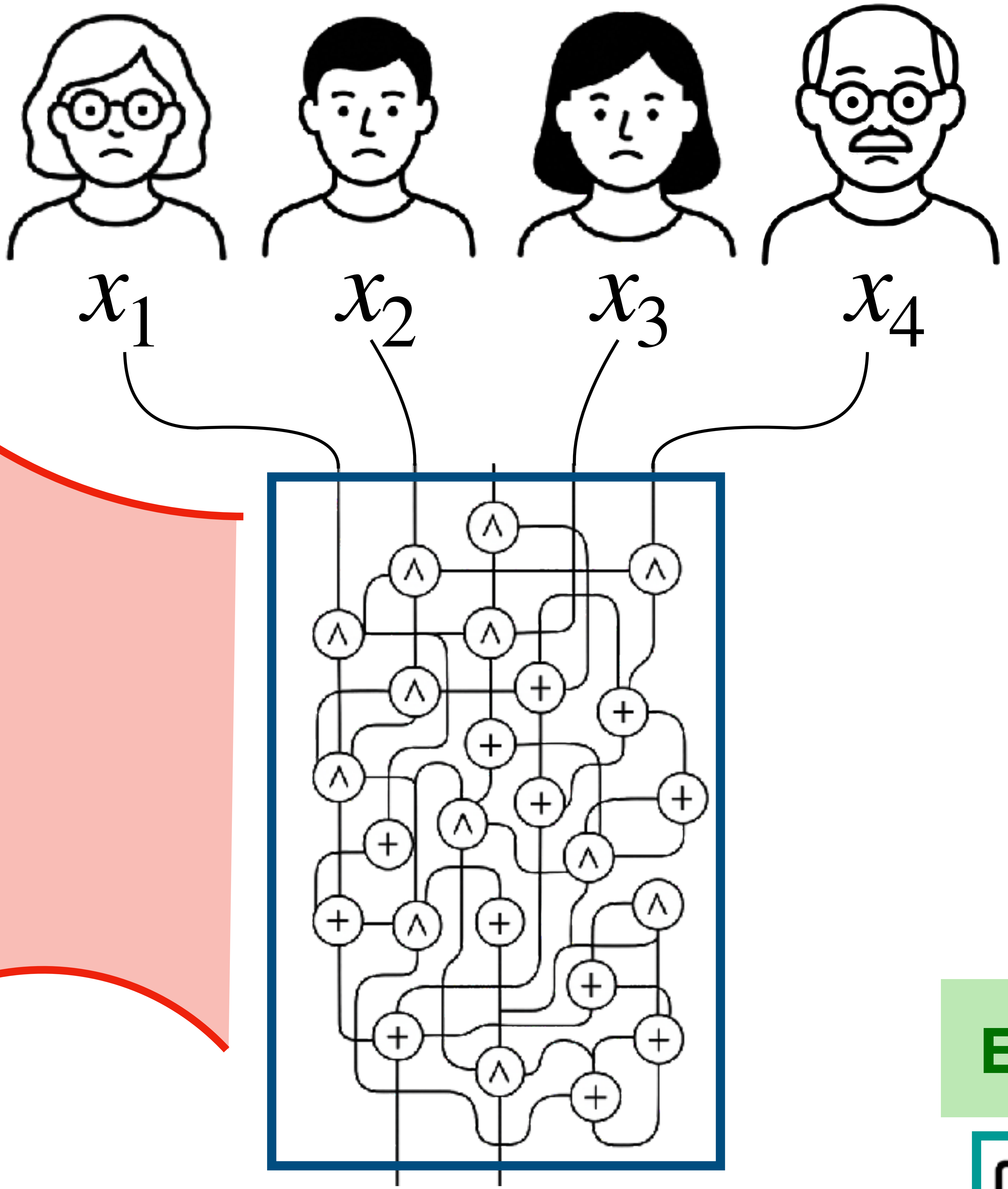
512 octets



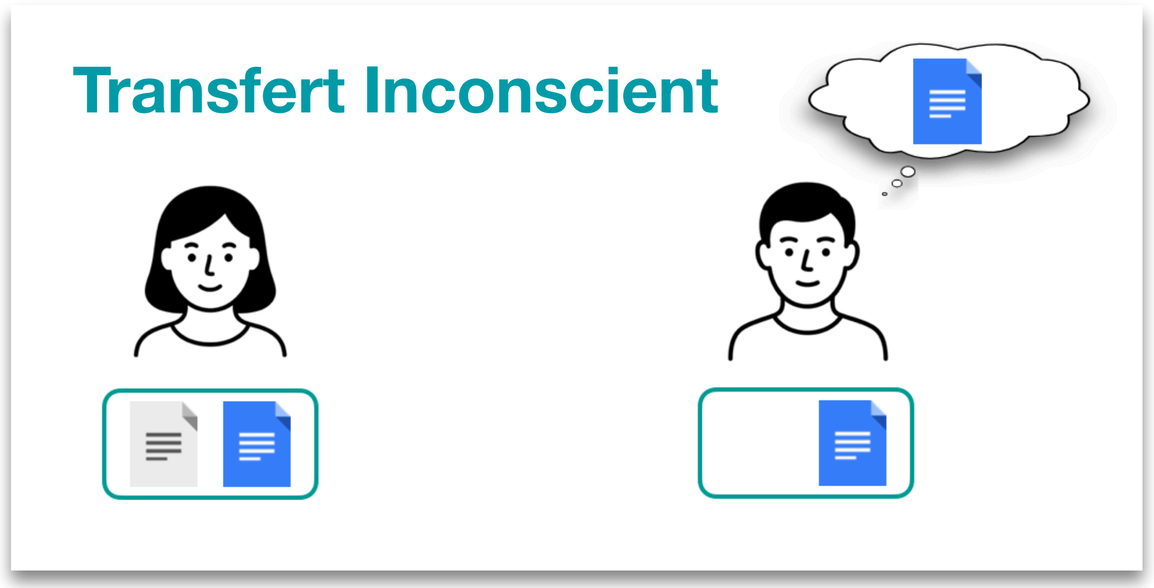
AAACGTACCTGACAAT
ACACGTACCTGACAAT
ACACGT_CCTGACAAT
ACACGTCTTGACAAT
8 ACACGTCTTGAGCAAT
ACGCGTCTTGAGCAAT
ACGCGTCTTGAGC_AT
ACGCGTCTTGAGC_T
TACGCGTCTTGAGCT

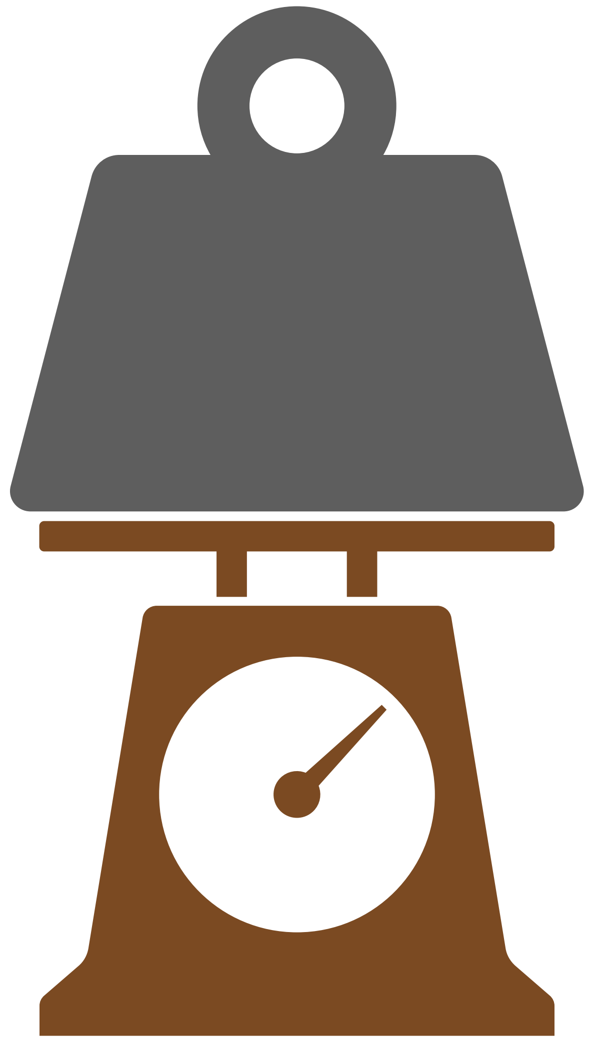


512 octets



5,901,194,475 portes





Exemple : distance d'édition

: 1200 heures

: 1.1 Téraoctet

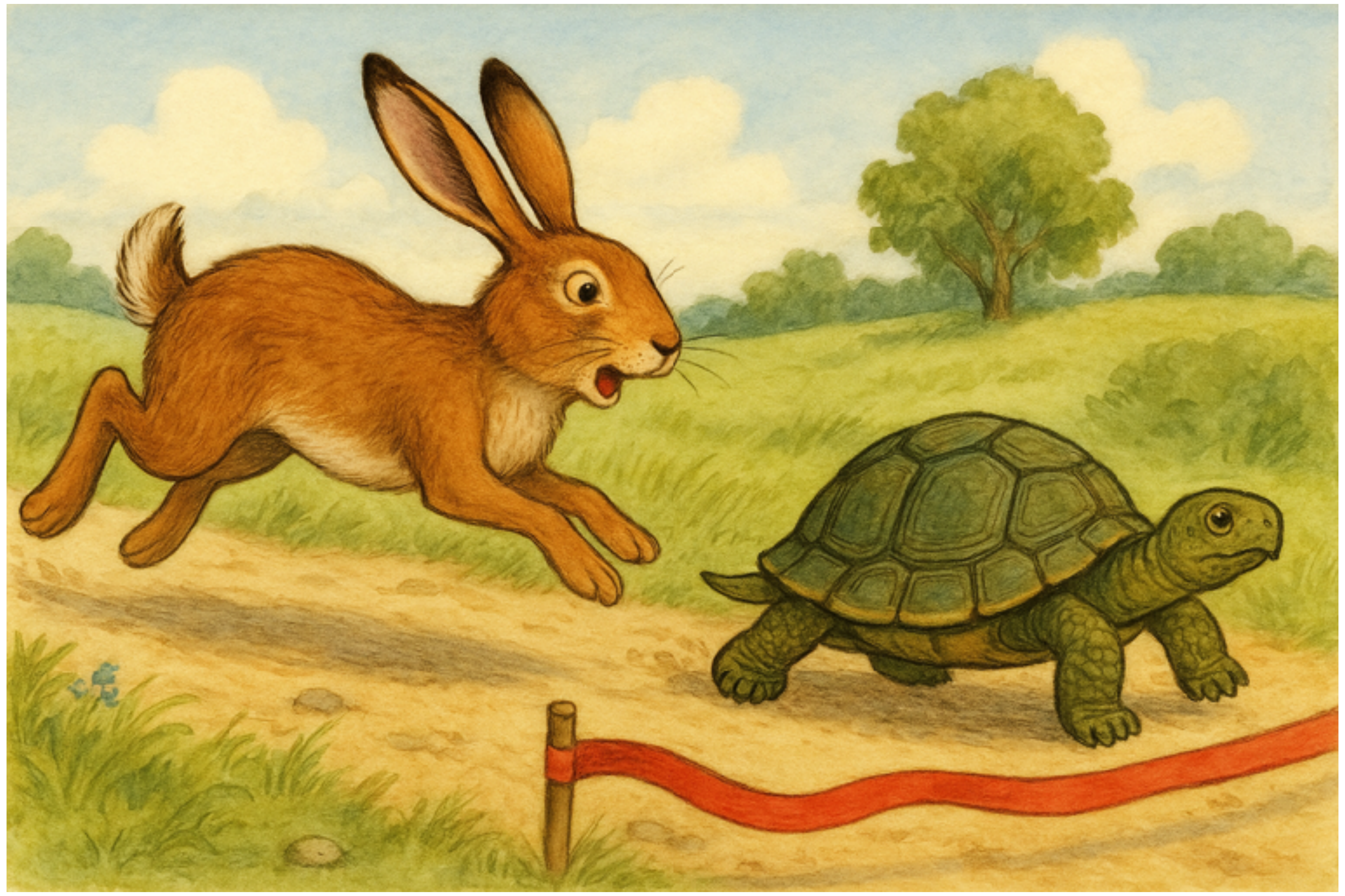
Transferts Inconscients : et s'il en faut plein ?

Problème : on ne sait pas faire un OT moins coûteux (et on a de bonnes raisons de croire que c'est très difficile)

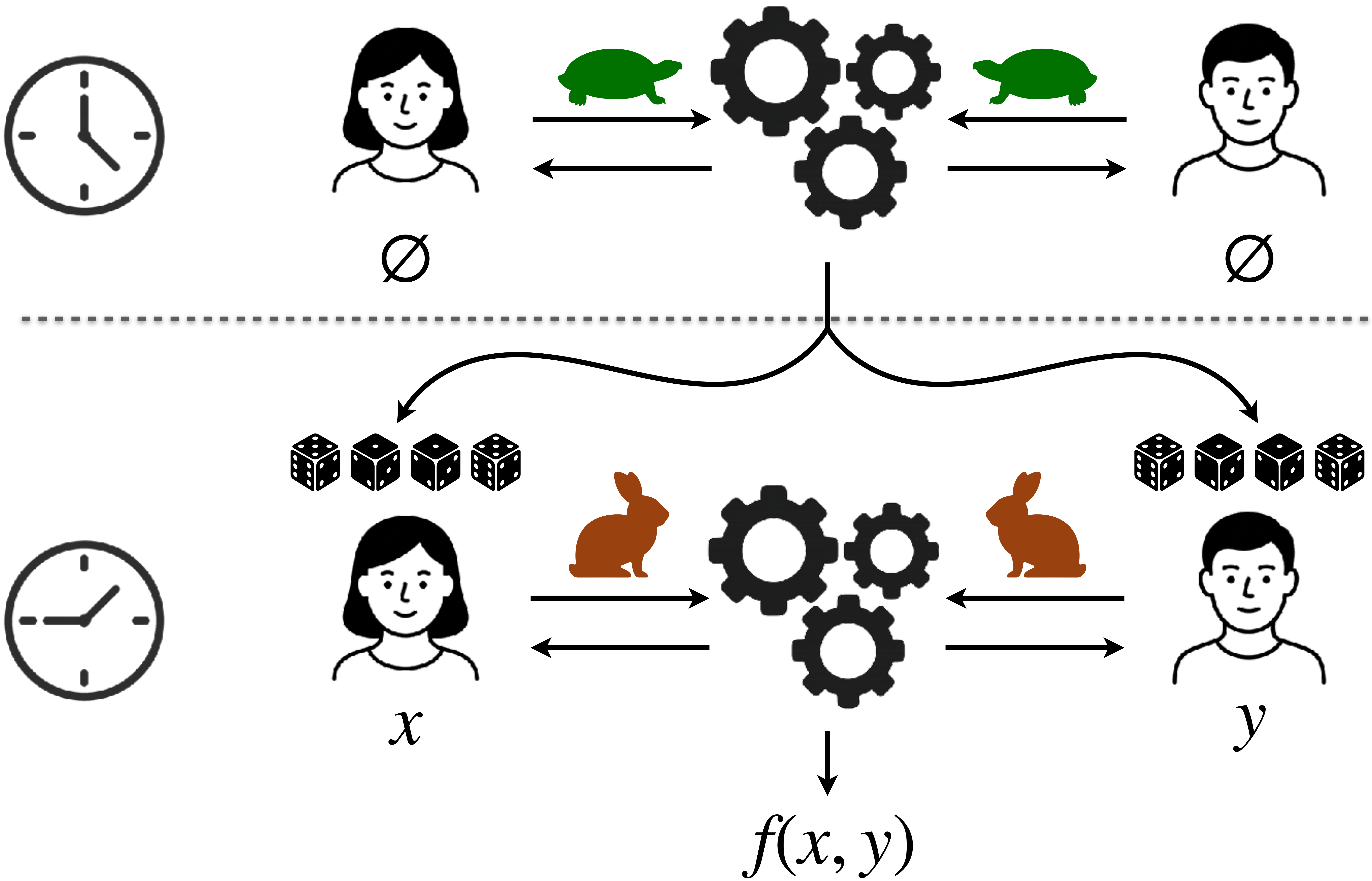
Transferts Inconscients : et s'il en faut plein ?

Problème : on ne sait pas faire un OT moins coûteux (et on a de bonnes raisons de croire que c'est très difficile)

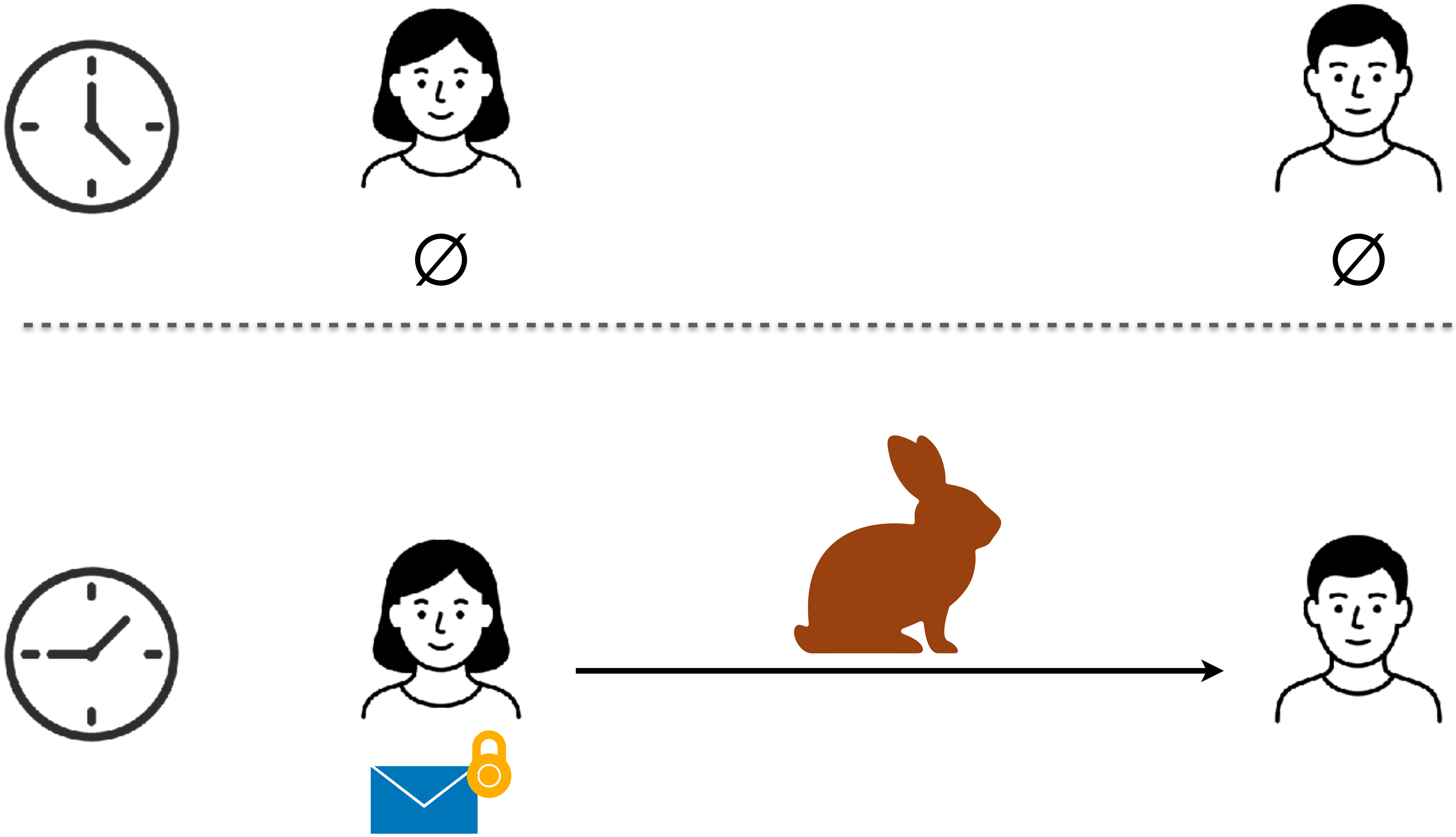
« Rien ne sert de courir, il faut partir à point. »



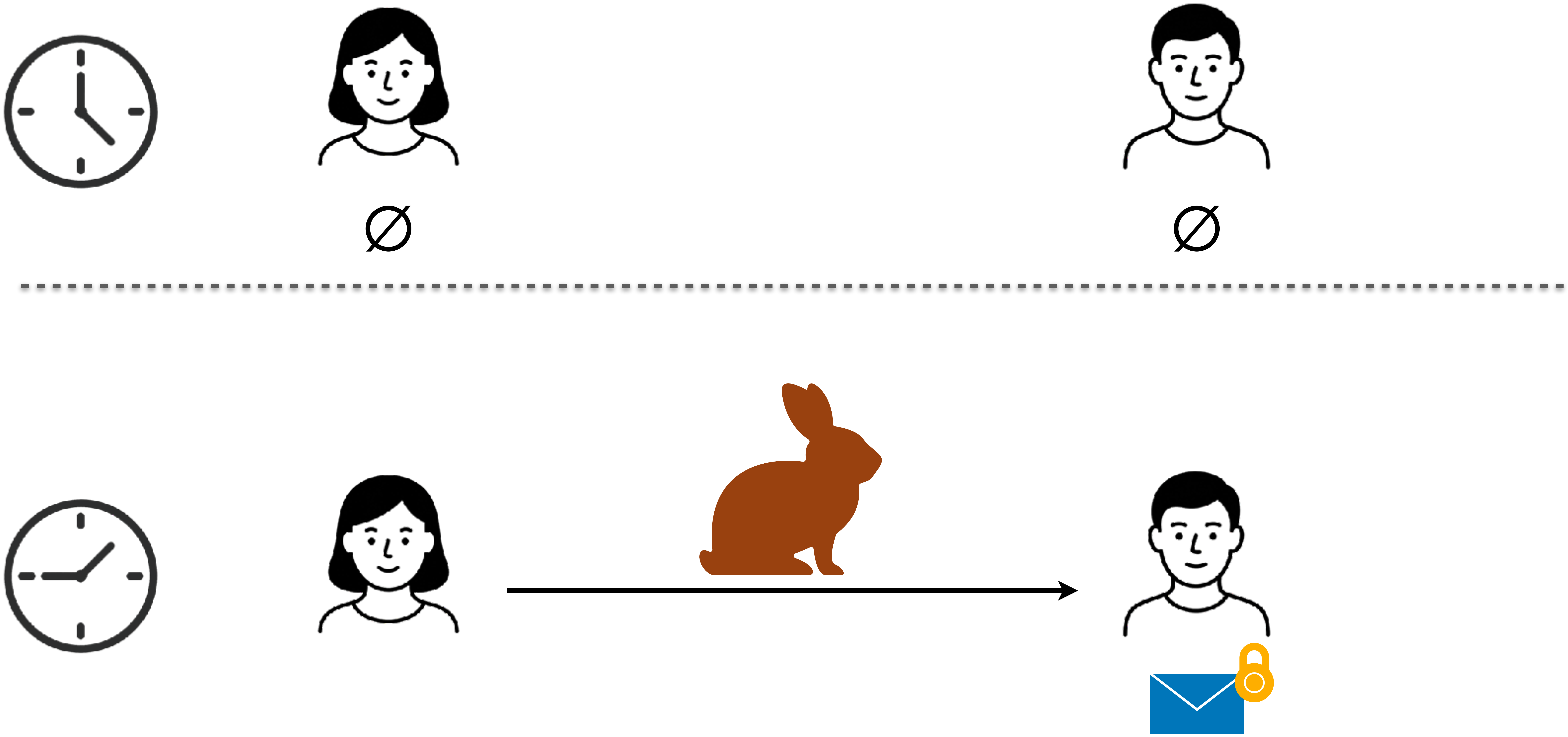
Préparer de l'aléa corrélé pour le calcul sécurisé



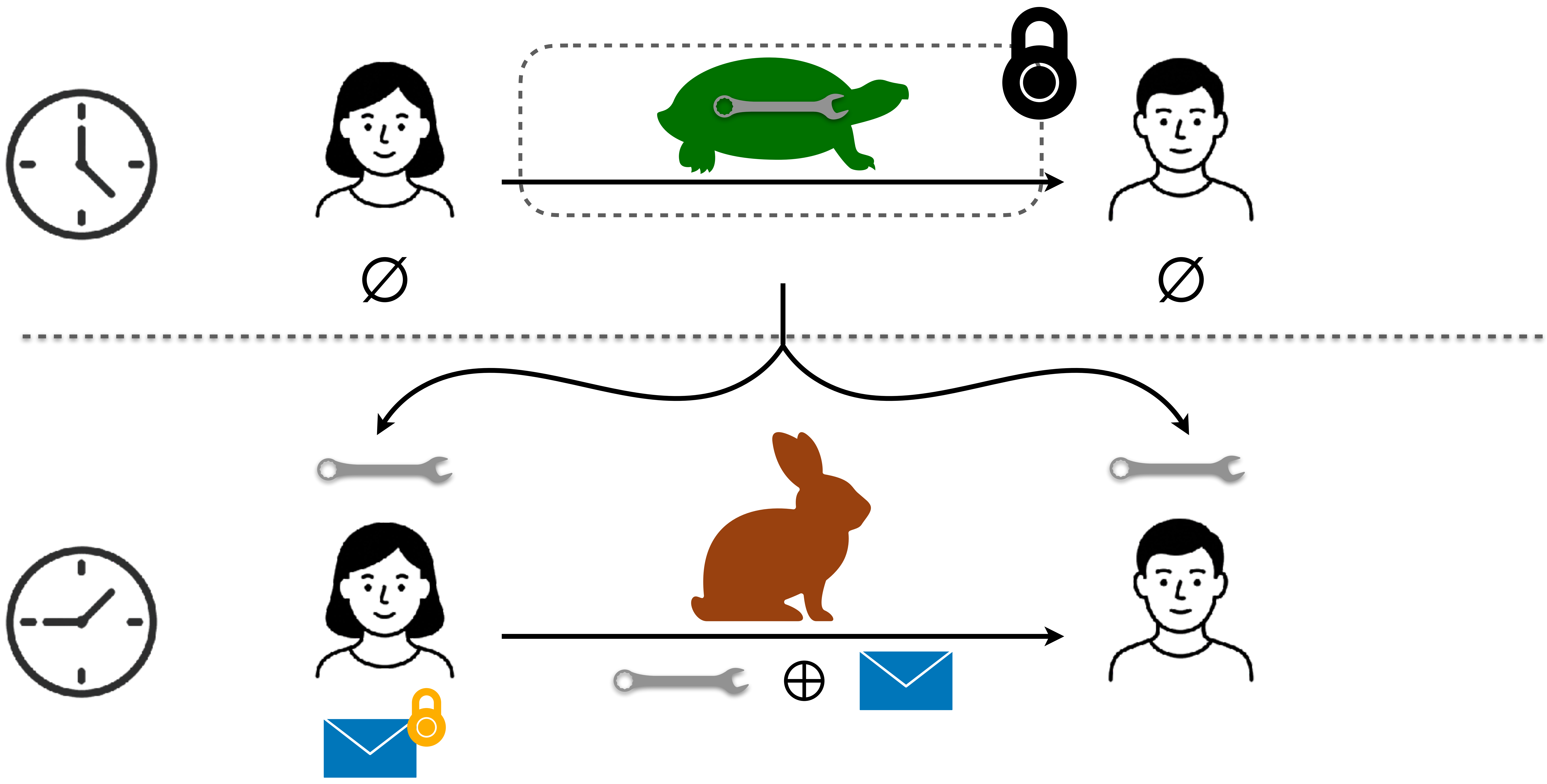
Interlude 0 : analogie avec le chiffre de Vernam



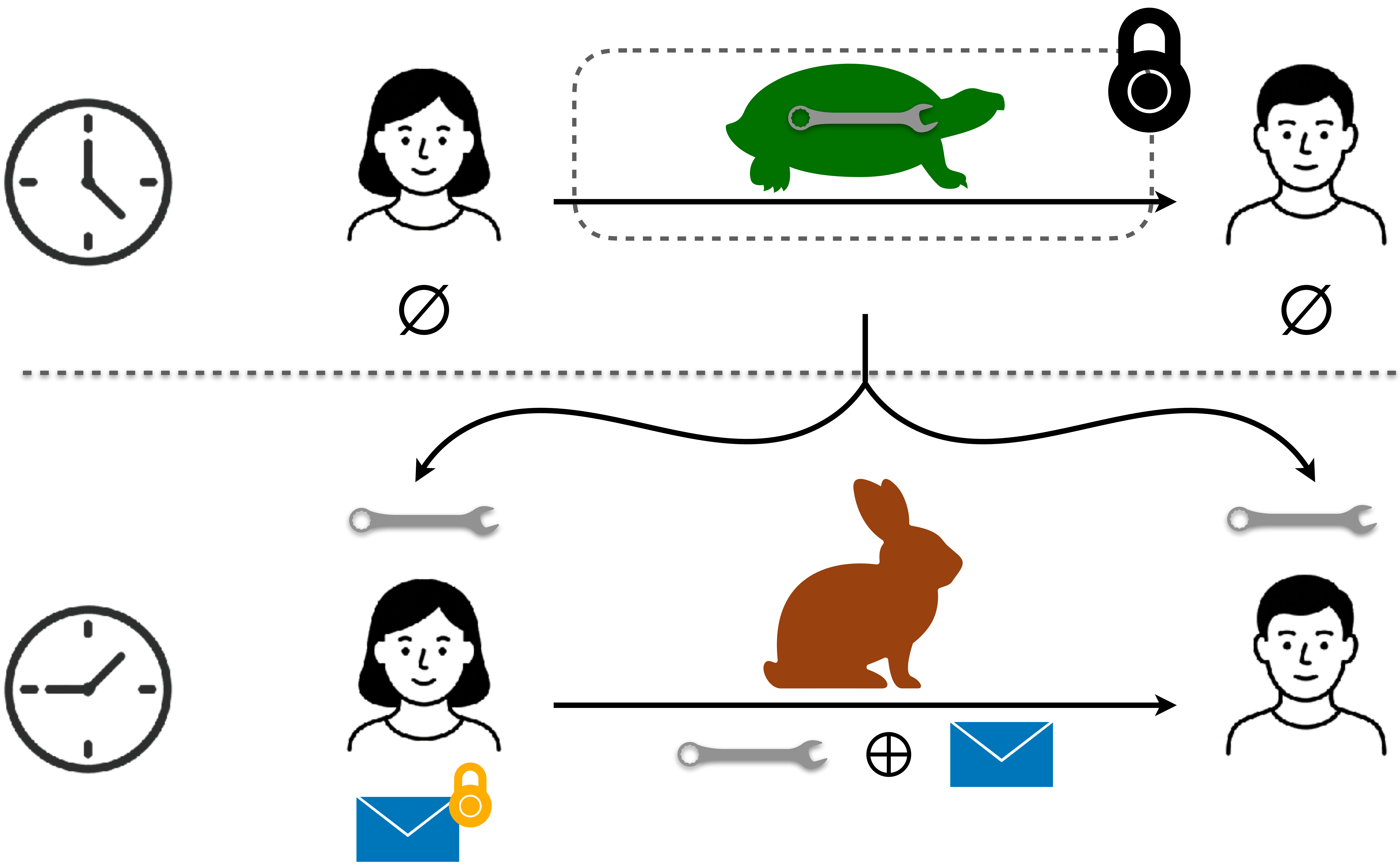
Interlude 0 : analogie avec le chiffre de Vernam



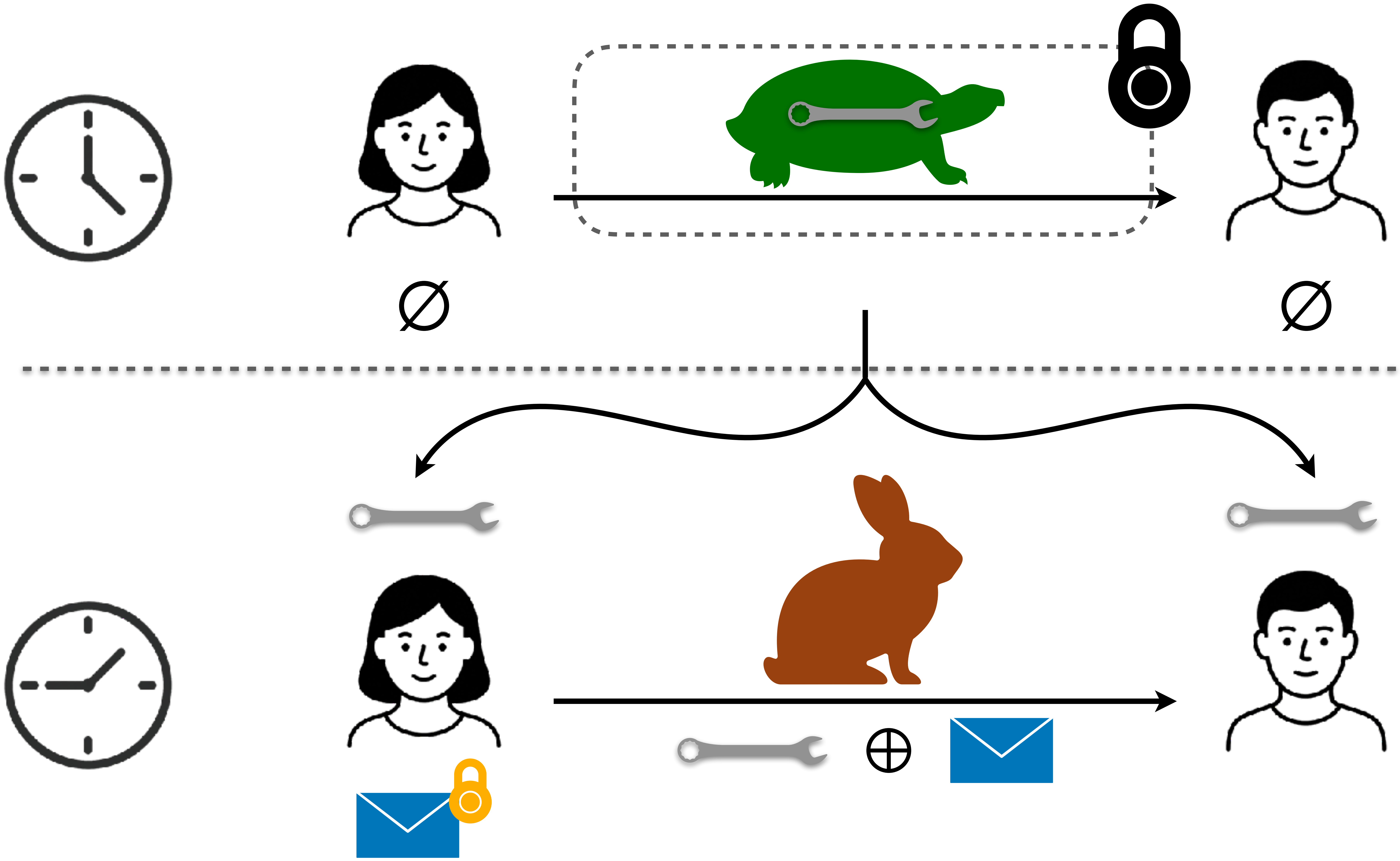
Interlude 0 : analogie avec le chiffre de Vernam



Interlude 0 : analogie avec le chiffre de Vernam



Interlude 0 : analogie avec le chiffre de Vernam



Préparer de l'aléa corrélé pour le calcul sécurisé

Aléa corrélé	Modèle		
ROT	GMW (Circuits Booléens, 2 joueurs, semi-honnête)	(r_0, r_1)	(σ, r_σ)
ROLE($\mathbb{F}$)	Circuits arithmétiques, 2 joueurs, semi-honnête	(u, v)	$(x, ux + v)$
Triplets authentifiés	Circuits arithmétiques, 2 joueurs, malicieux	Parts additives $\langle a, b, ab, \Delta a, \Delta b, \Delta ab \rangle$ pour un MAC Δ	
Triplets matriciels	Algèbre linéaire, 2 joueurs, semi-honnête	Parts additives $\langle A, B, A \cdot B \rangle$	
Autres : corrélations de haut degré, tables de vérité à usage unique, parts de vecteurs unitaires…	Divers protocoles spécialisés : requêtes à une BDD, statistiques…	(Divers)	

Préparer de l’aléa corrélé pour le calcul sécurisé

Aléa corrélé	**Modèle**		
ROT	GMW (Circuits Booléens, 2 joueurs, semi-honnête)	(r_0, r_1)	(σ, r_σ)
ROLE($\mathbb{F}$)	Circuits arithmétiques, 2 joueurs, semi-honnête	(u, v)	$(x, ux + v)$
Triplets authentifiés	Circuits arithmétiques, 2 joueurs, malicieux	Parts additives $\langle a, b, ab, \Delta a, \Delta b, \Delta ab\rangle$ pour un MAC Δ	
Triplets matriciels	Algèbre linéaire, 2 joueurs, semi-honnête	Parts additives $\langle A, B, A \cdot B\rangle$	
Autres : corrélations de haut degré, tables de vérité à usage unique, parts de vecteurs unitaires…	Divers protocoles spécialisés : requêtes à une BDD, statistiques…	(Divers)	

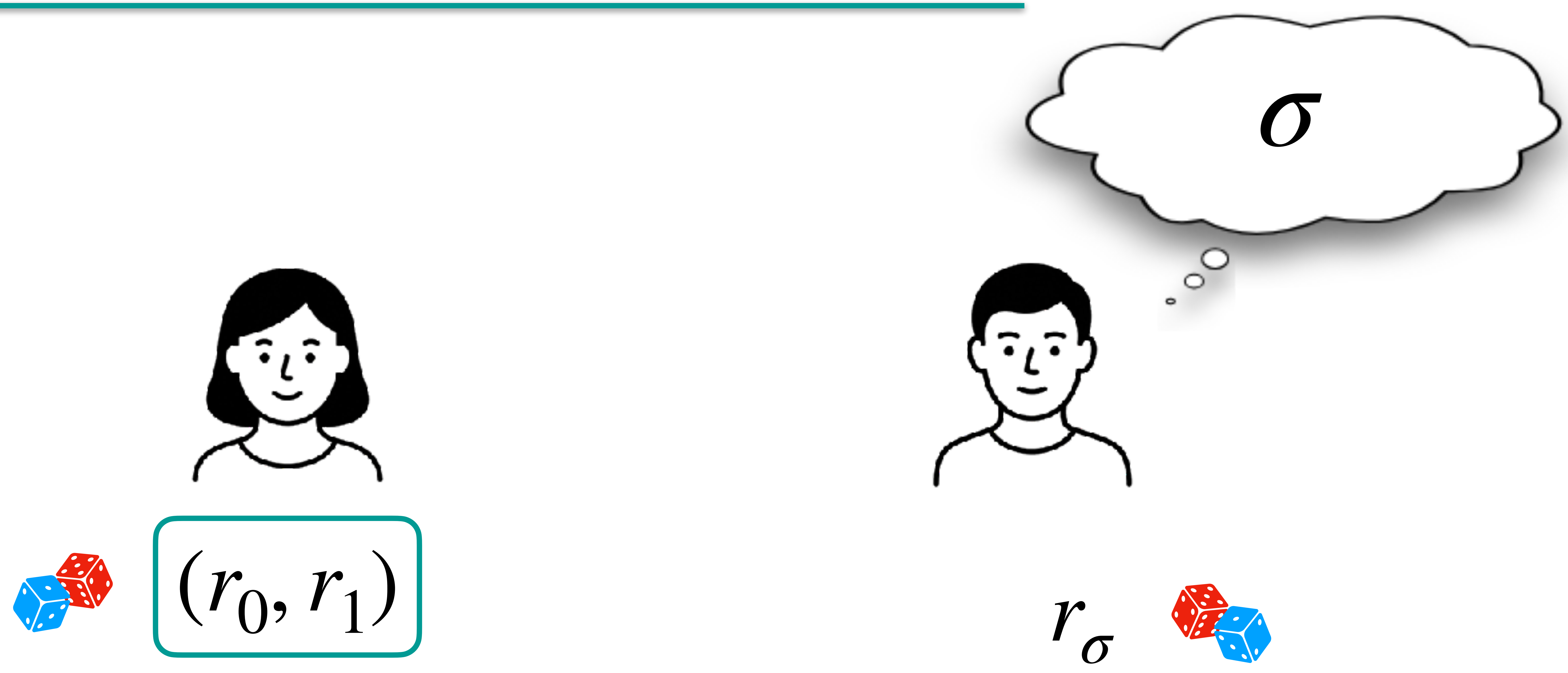
Transferts Inconscients : préparation anticipée

RAPPEL DE COURS

Transferts Inconscients : préparation anticipée

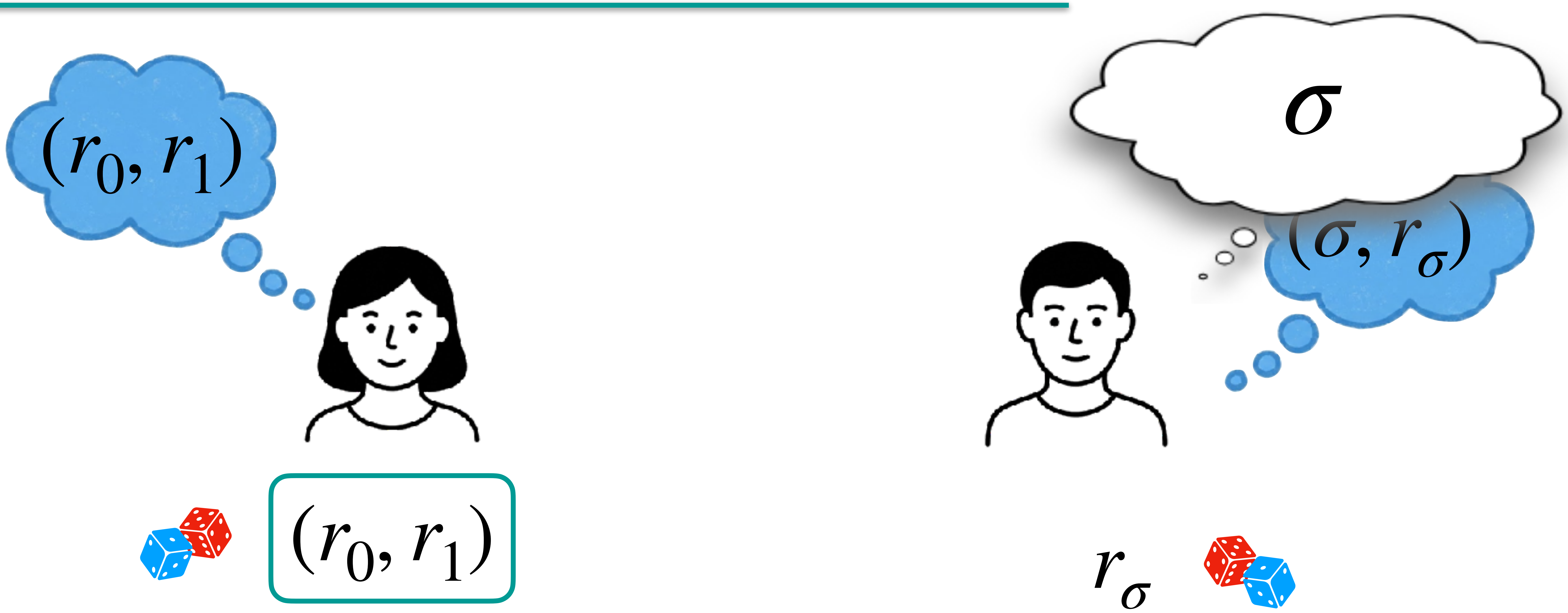
Transferts Inconscients : préparation anticipée

RAPPEL DE COURS



Transferts Inconscients : préparation anticipée

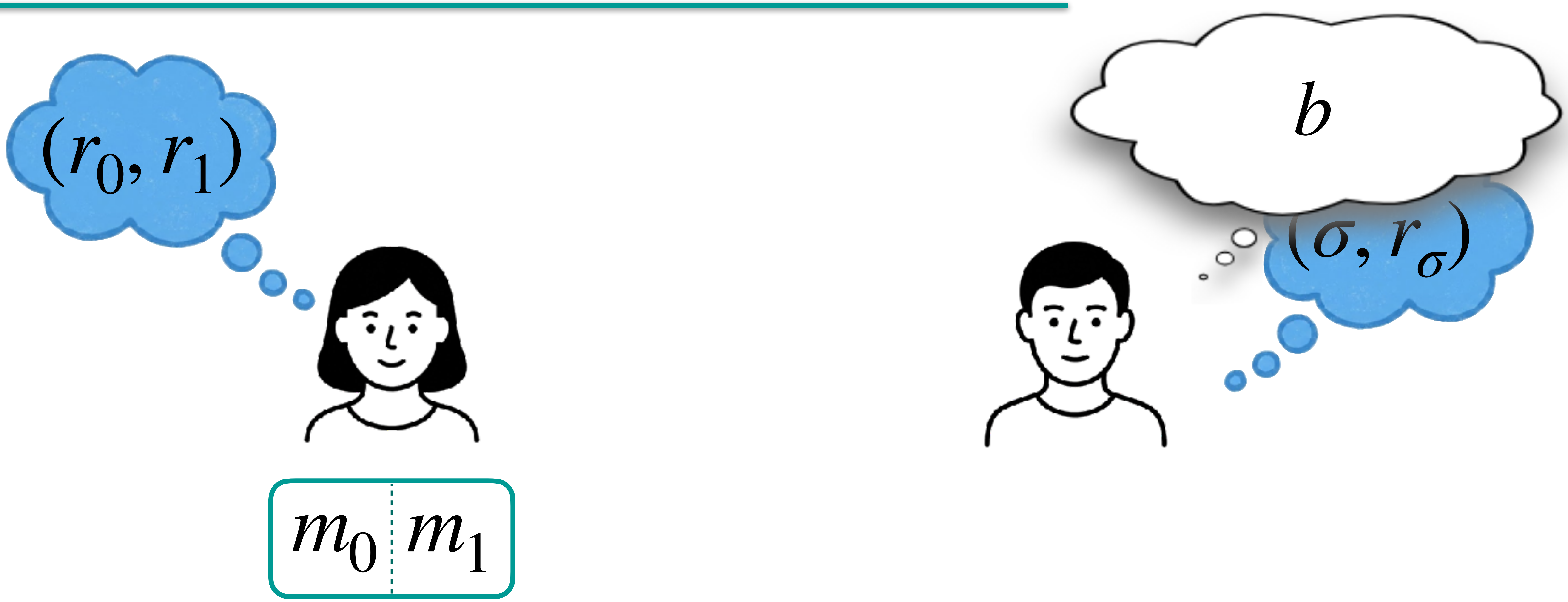
RAPPEL DE COURS



Transferts Inconscients : préparation anticipée

Beaver, 1991

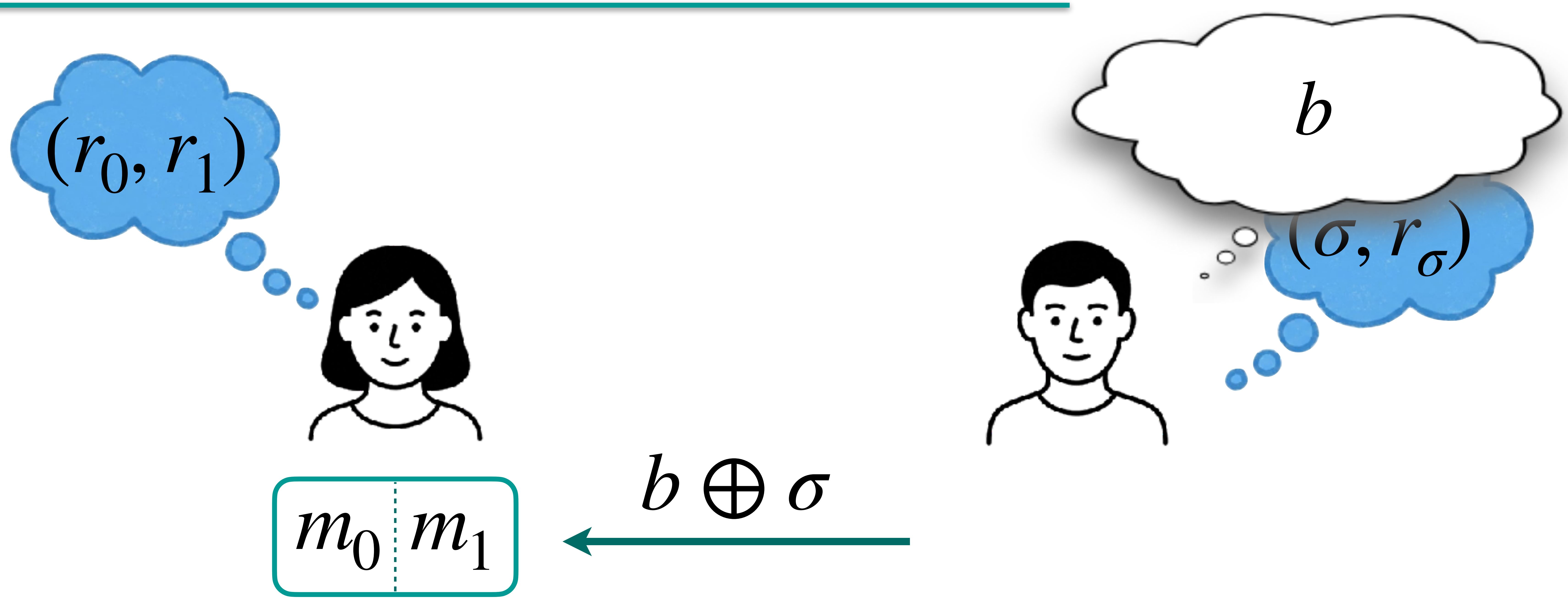
RAPPEL DE COURS



Transferts Inconscients : préparation anticipée

Beaver, 1991

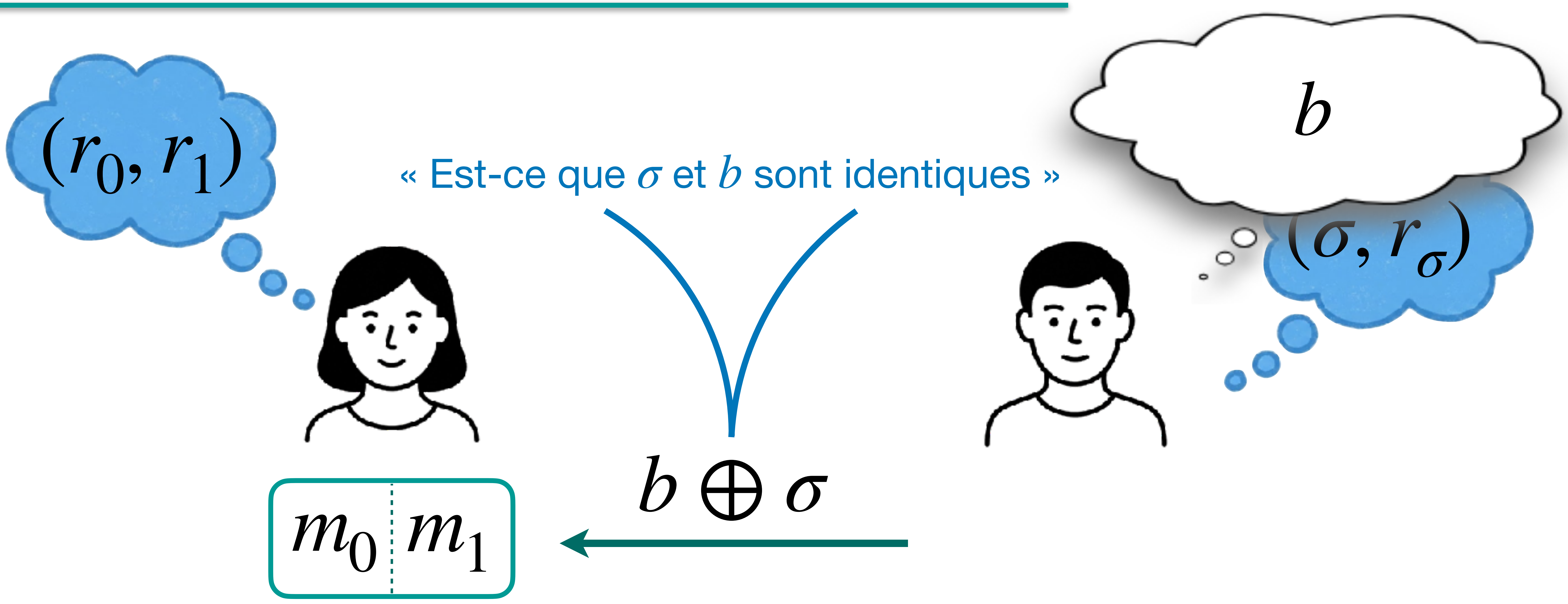
RAPPEL DE COURS



Transferts Inconscients : préparation anticipée

Beaver, 1991

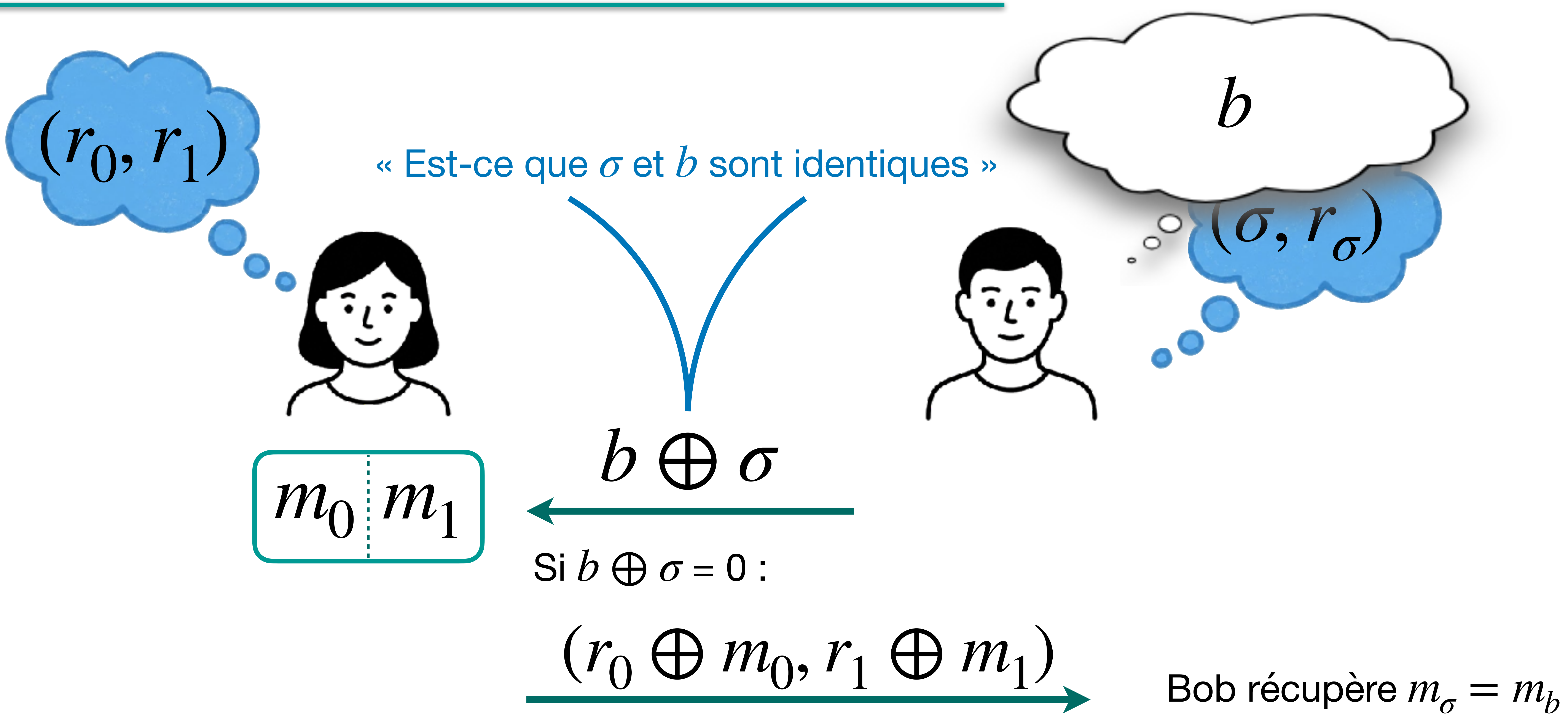
RAPPEL DE COURS



Transferts Inconscients : préparation anticipée

Beaver, 1991

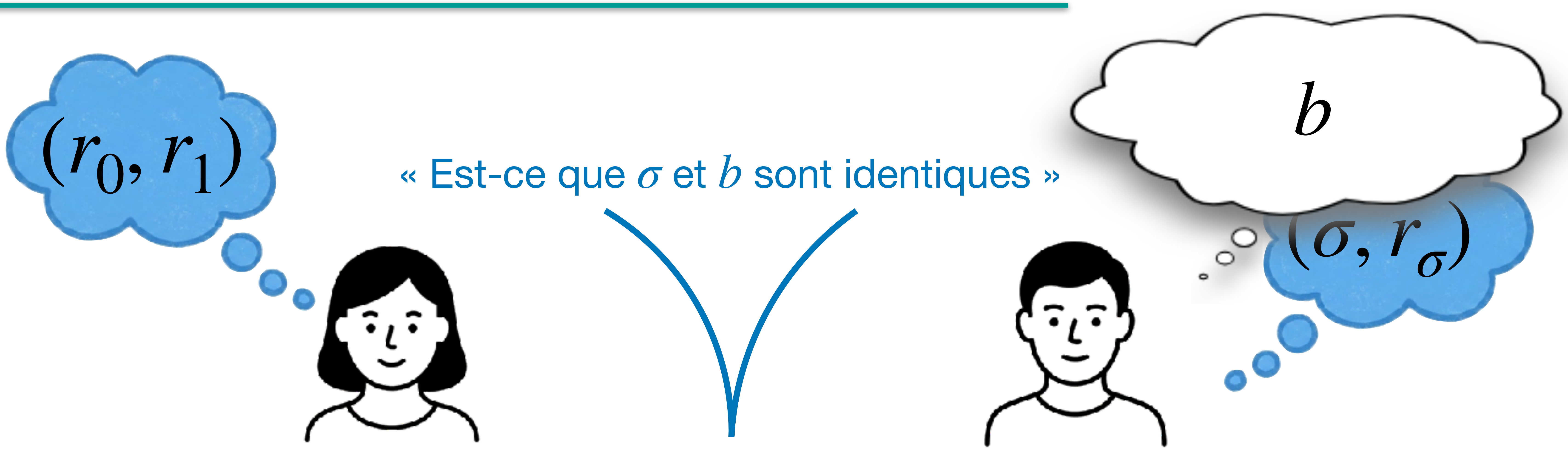
RAPPEL DE COURS



Transferts Inconscients : préparation anticipée

Beaver, 1991

RAPPEL DE COURS



$m_0 \mid m_1$

$$\xleftarrow{\;b \oplus \sigma\;}$$

Si $b \oplus \sigma = 0$:

$$\xrightarrow{\;(r_0 \oplus m_0, r_1 \oplus m_1)\;}$$

Bob récupère $m_\sigma = m_b$

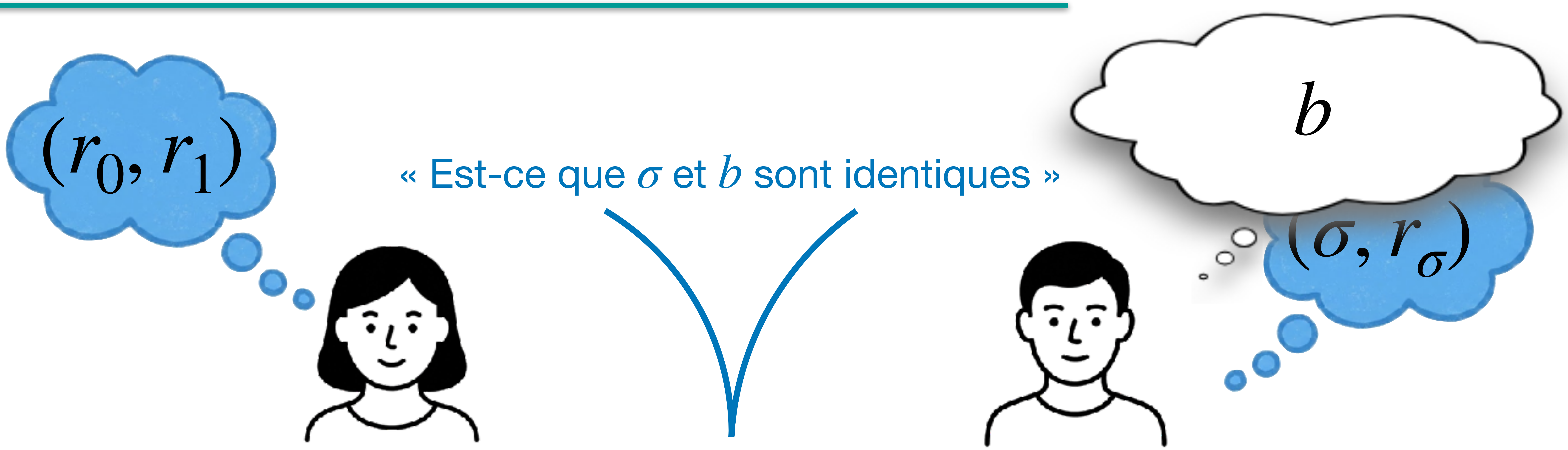
Si $b \oplus \sigma = 1$:

$$\xrightarrow{\;(r_1 \oplus m_0, r_0 \oplus m_1)\;}$$

Bob récupère $m_{1-\sigma} = m_b$

Transferts Inconscients : préparation anticipée

Beaver, 1991



$m_0 \mid m_1$

$\xleftarrow{\;b \oplus \sigma\;}$

Si $b \oplus \sigma = 0$:

$\xrightarrow{(r_0 \oplus m_0, r_1 \oplus m_1)}$ Bob récupère $m_\sigma = m_b$

Si $b \oplus \sigma = 1$:

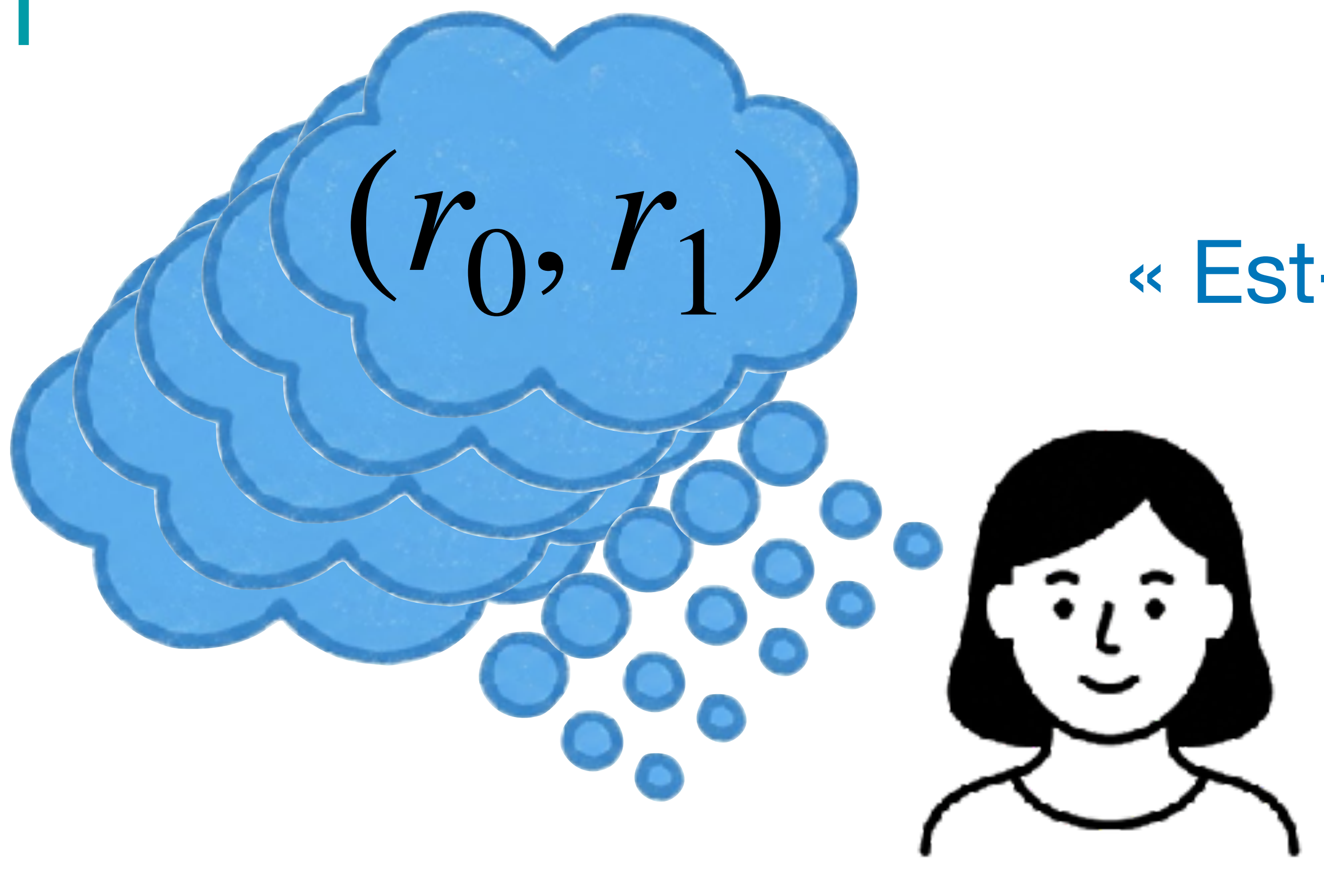
$\xrightarrow{(r_1 \oplus m_0, r_0 \oplus m_1)}$ Bob récupère $m_{1-\sigma} = m_b$

Conclusion : si on précalcule un transfert sur des bits aléatoires, on peut le « dérandomiser » inconditionnellement, pour trois bits de communication et quelques XORs

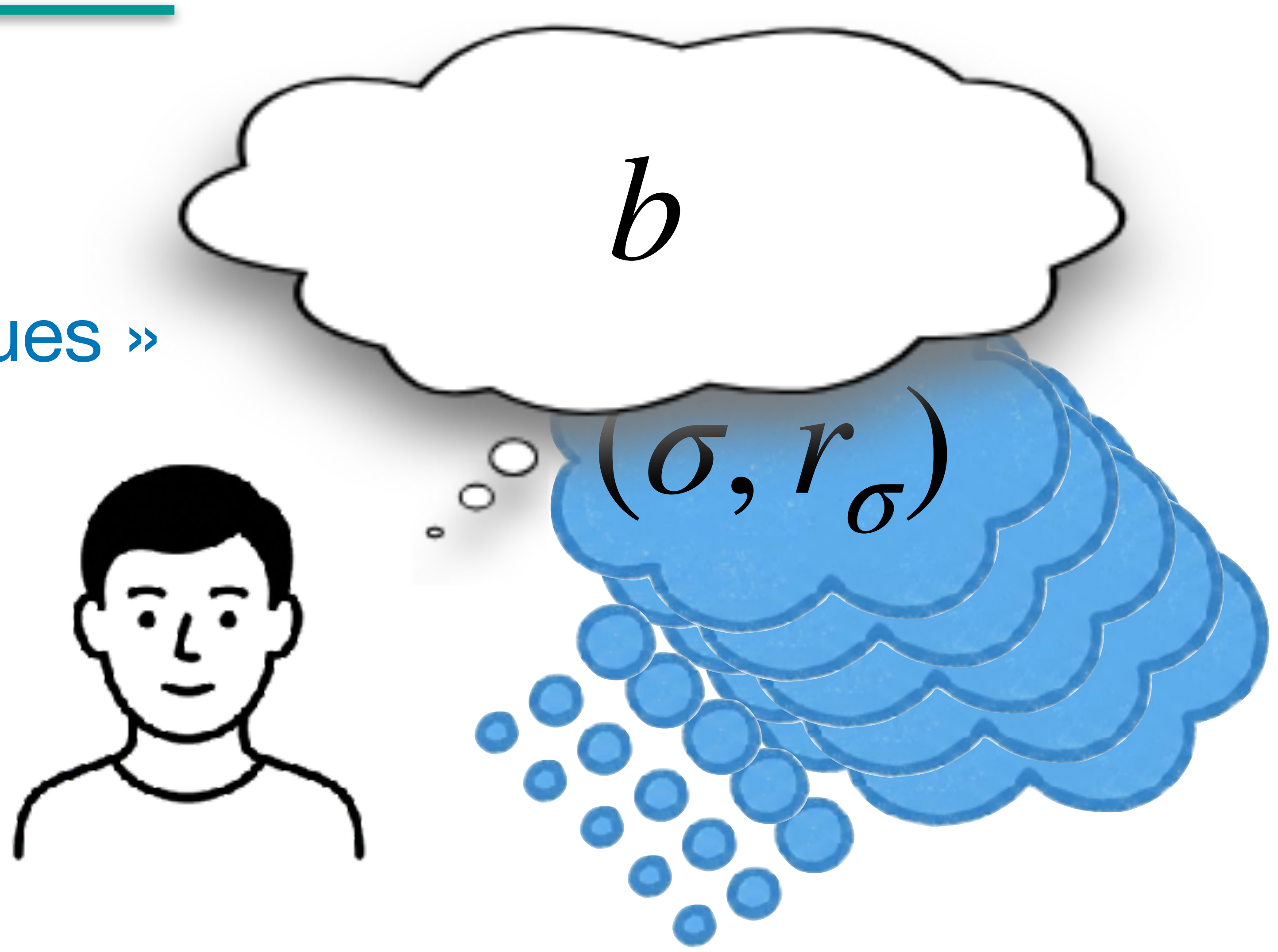
Transferts Inconscients : préparation anticipée

Beaver, 1991

RAPPEL DE COURS



« Est-ce que σ et b sont identiques »



$m_0 \mid m_1$

$\xleftarrow{b \oplus \sigma}$

Si $b \oplus \sigma = 0$:

$\xrightarrow{(r_0 \oplus m_0, r_1 \oplus m_1)}$ Bob récupère $m_\sigma = m_b$

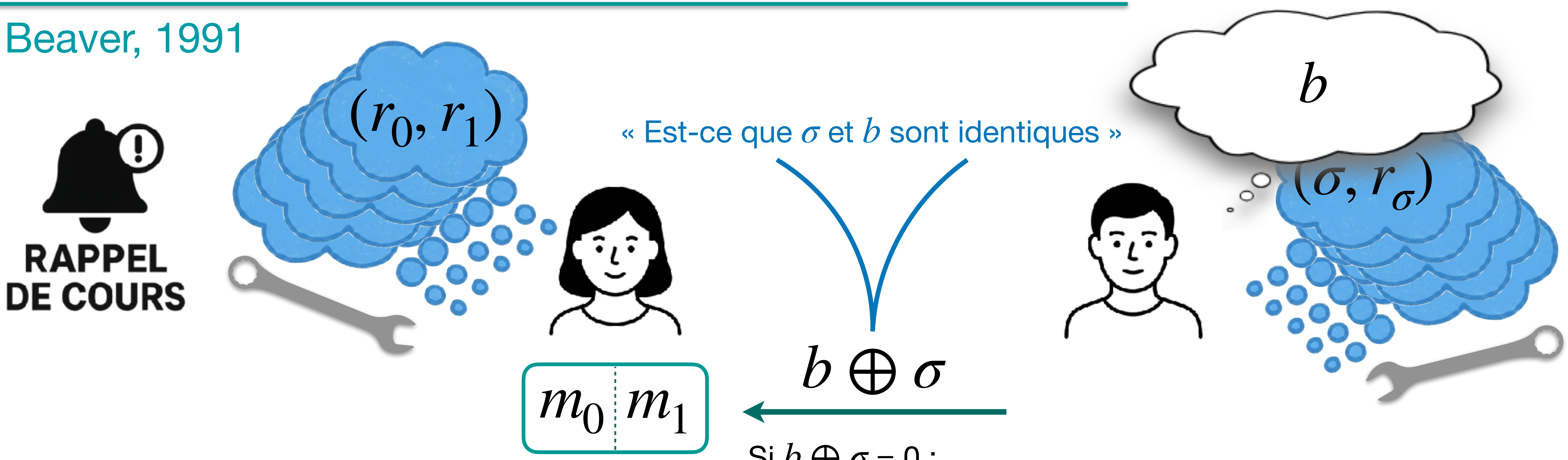
Si $b \oplus \sigma = 1$:

$\xrightarrow{(r_1 \oplus m_0, r_0 \oplus m_1)}$ Bob récupère $m_{1-\sigma} = m_b$

Conclusion : si on précalcule un transfert sur des bits aléatoires, on peut le « dérandomiser » inconditionnellement, pour trois bits de communication et quelques XORs

Transferts Inconscients : préparation anticipée

Beaver, 1991



Si $b \oplus \sigma = 0$:

$(r_0 \oplus m_0, r_1 \oplus m_1)$ → Bob récupère $m_\sigma = m_b$

Si $b \oplus \sigma = 1$:

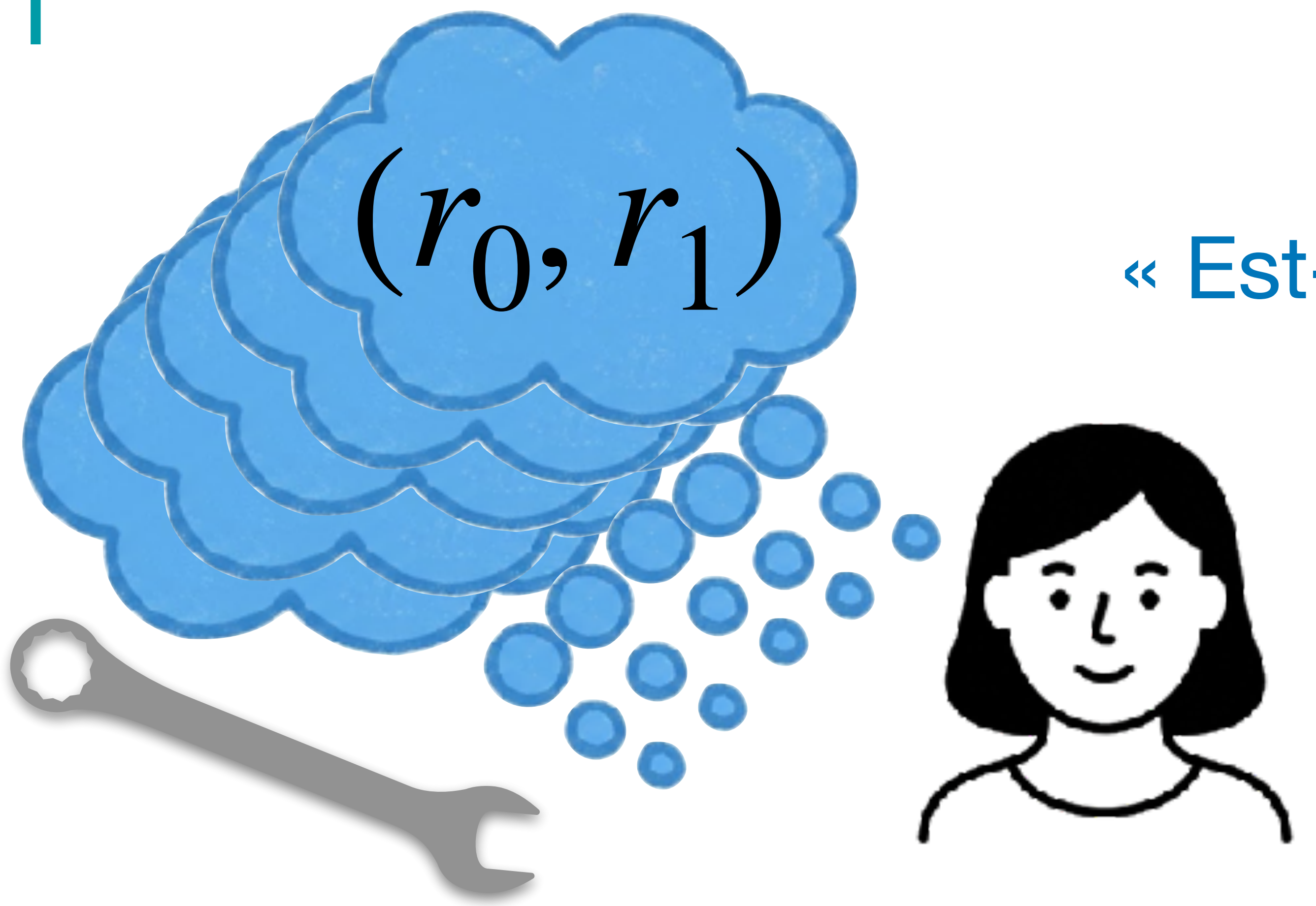
$(r_1 \oplus m_0, r_0 \oplus m_1)$ → Bob récupère $m_{1-\sigma} = m_b$

Conclusion : si on précalcule un transfert sur des bits aléatoires, on peut le « dérandomiser » inconditionnellement, pour trois bits de communication et quelques XORs

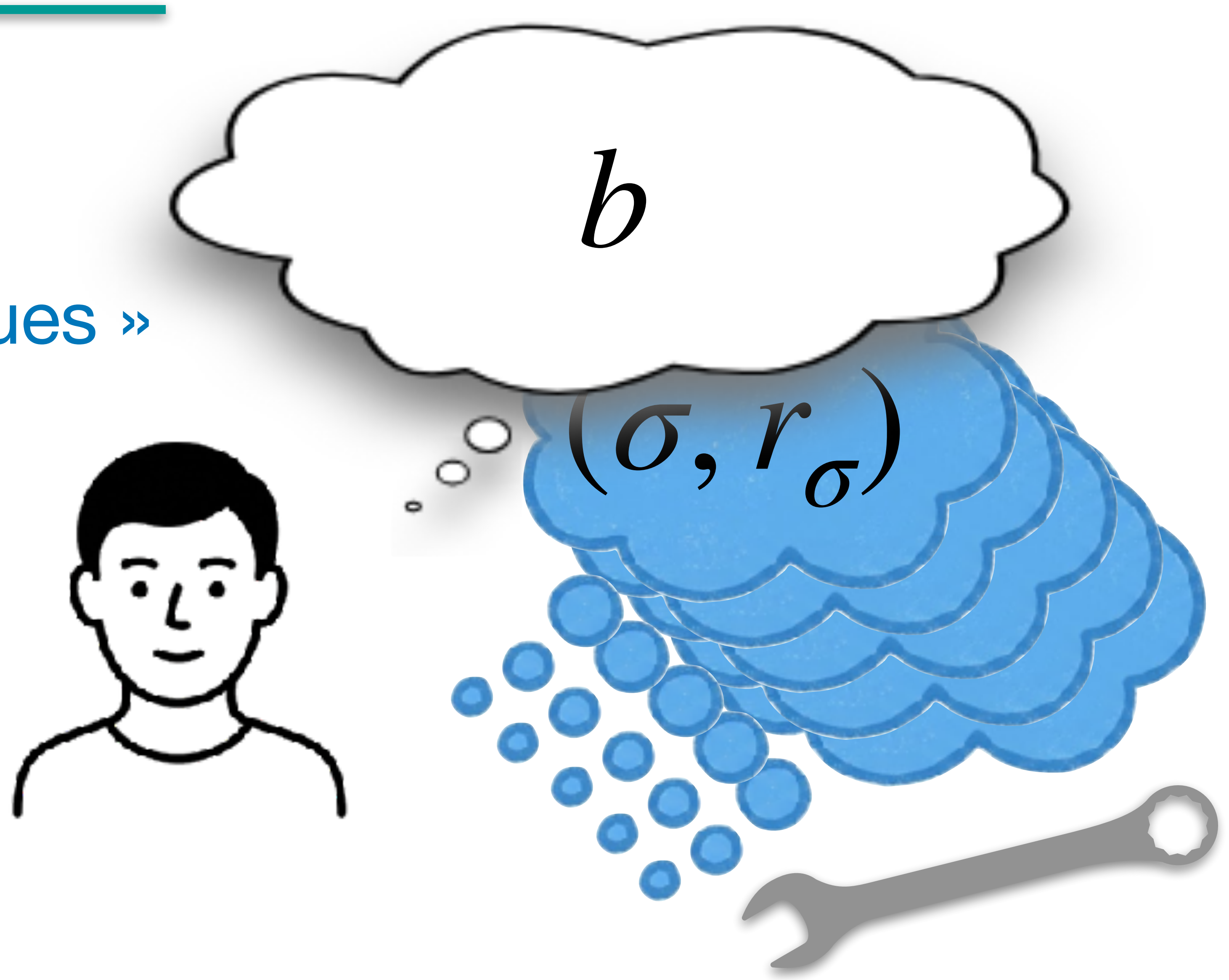
Transferts Inconscients : préparation anticipée

Beaver, 1991

RAPPEL DE COURS



« Est-ce que σ et b sont identiques »



$m_0 \mid m_1$

$\xleftarrow{\quad b \oplus \sigma \quad}$

Si $b \oplus \sigma = 0$:

$\xrightarrow{(r_0 \oplus m_0, r_1 \oplus m_1)}$ Bob récupère $m_\sigma = m_b$

Si $b \oplus \sigma = 1$:

$\xrightarrow{(r_1 \oplus m_0, r_0 \oplus m_1)}$ Bob récupère $m_{1-\sigma} = m_b$

Conclusion : si on précalcule un transfert sur des bits aléatoires, on peut le « dérandomiser » inconditionnellement, pour trois bits de communication et quelques XORs

: ~ $67 \cdot 10^9$/s (2.4 GHz)

: 6 bits/porte

Transferts Inconscients : préparation anticipée

Beaver, 1991

RAPPEL DE COURS

(r_0, r_1)

« Est-ce que σ et b sont identiques »

b

(σ, r_σ)

$m_0 \mid m_1$

$b \oplus \sigma$

Si $b \oplus \sigma = 0$:

$(r_0 \oplus m_0, r_1 \oplus m_1)$

Bob récupère $m_\sigma = m_b$

Si $b \oplus \sigma = 1$:

$(r_1 \oplus m_0, r_0 \oplus m_1)$

Bob récupère $m_{1-\sigma} = m_b$

Conclusion : si on précalcule un transfert sur des bits aléatoires, on peut le « dérandomiser » inconditionnellement, pour trois bits de communication et quelques XORs

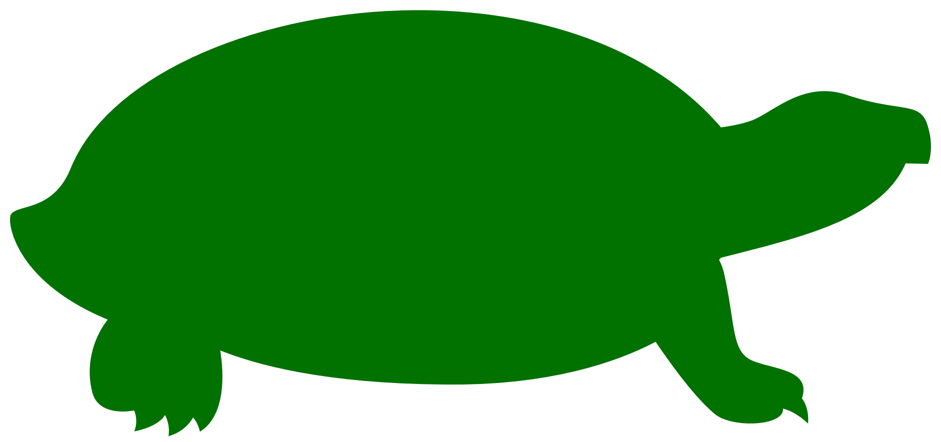
: 1200 heures

: 1.1 Téraoctet

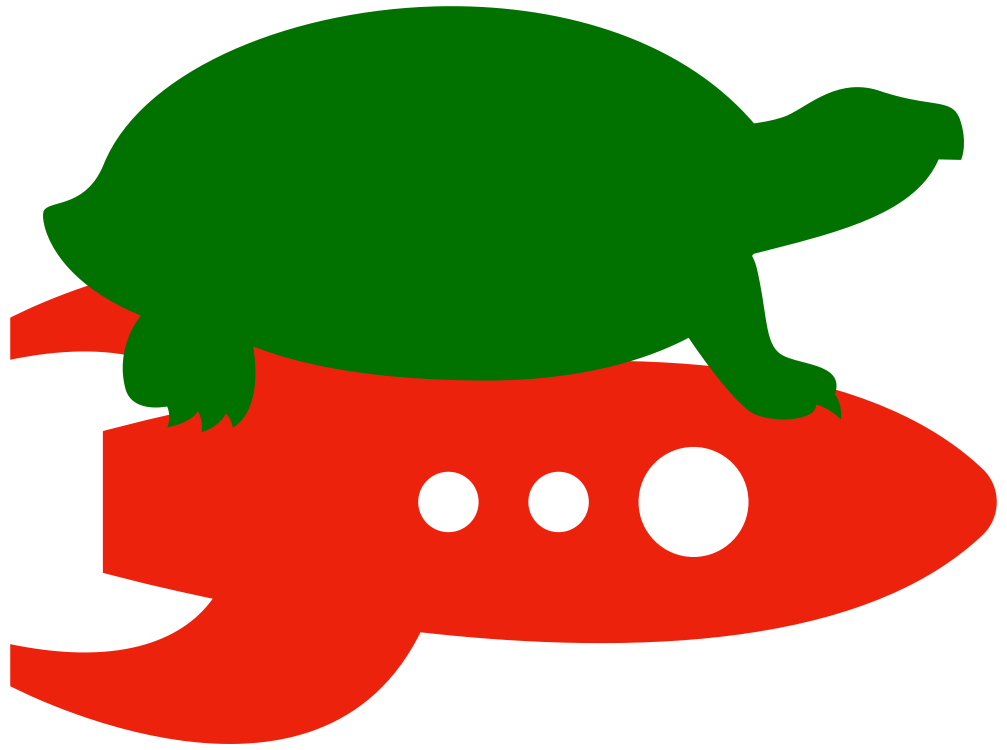
: ~ $67 \cdot 10^9$/s (2.4 GHz)

: 6 bits/porte

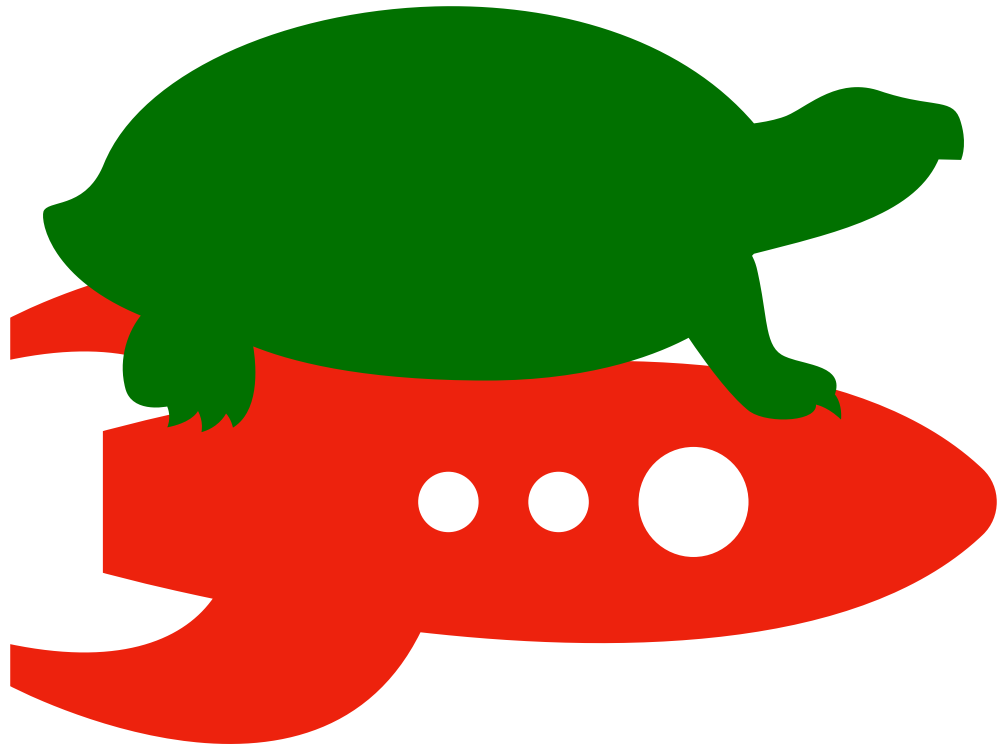
Transferts Inconscients aléatoires : une recette



Transferts Inconscients aléatoires : une recette

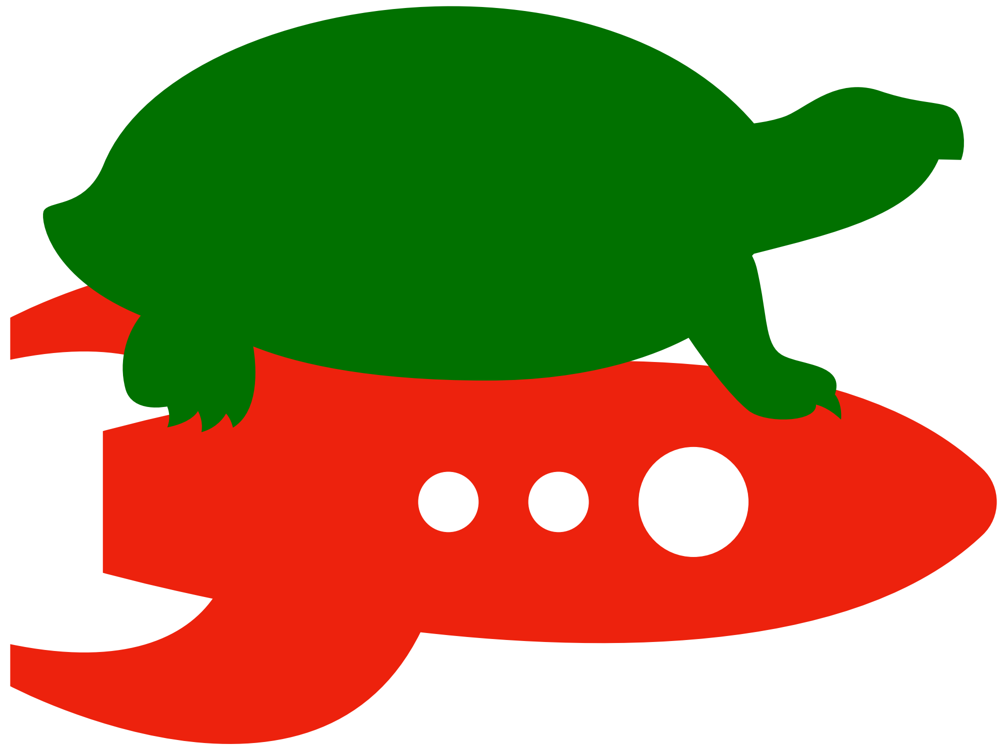


Transferts Inconscients aléatoires : une recette



1 Transferts inconscients « corrélés » (COT) $\Longrightarrow$ ROT

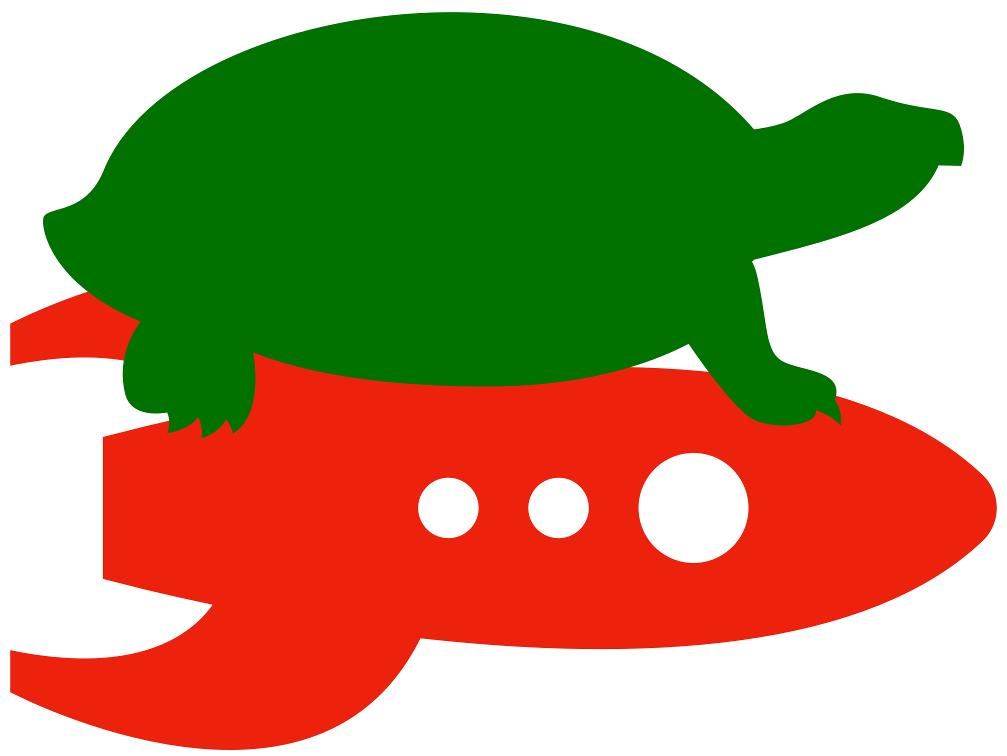
Transferts Inconscients aléatoires : une recette



1. Transferts inconscients « corrélés » (COT) $\Longrightarrow$ ROT

2. Quelques OTs + un PRG $\Longrightarrow$ COT

Transferts Inconscients aléatoires : une recette



1. Transferts inconscients « corrélés » (COT) $\Longrightarrow$ ROT

2. Quelques OTs + un PRG $\Longrightarrow$ COT

3. Si le PRG est *presque homomorphe*, on peut le faire… Presque sans communication !

Extension de transferts inconscients

Objectif : construire un grand nombre de OT à faible coût à partir d'un petit nombre de OT coûteux

Extension de transfers inconscients

Objectif : construire un grand nombre de OT à faible coût à partir d'un petit nombre de OT coûteux

Extension de transferts inconscients

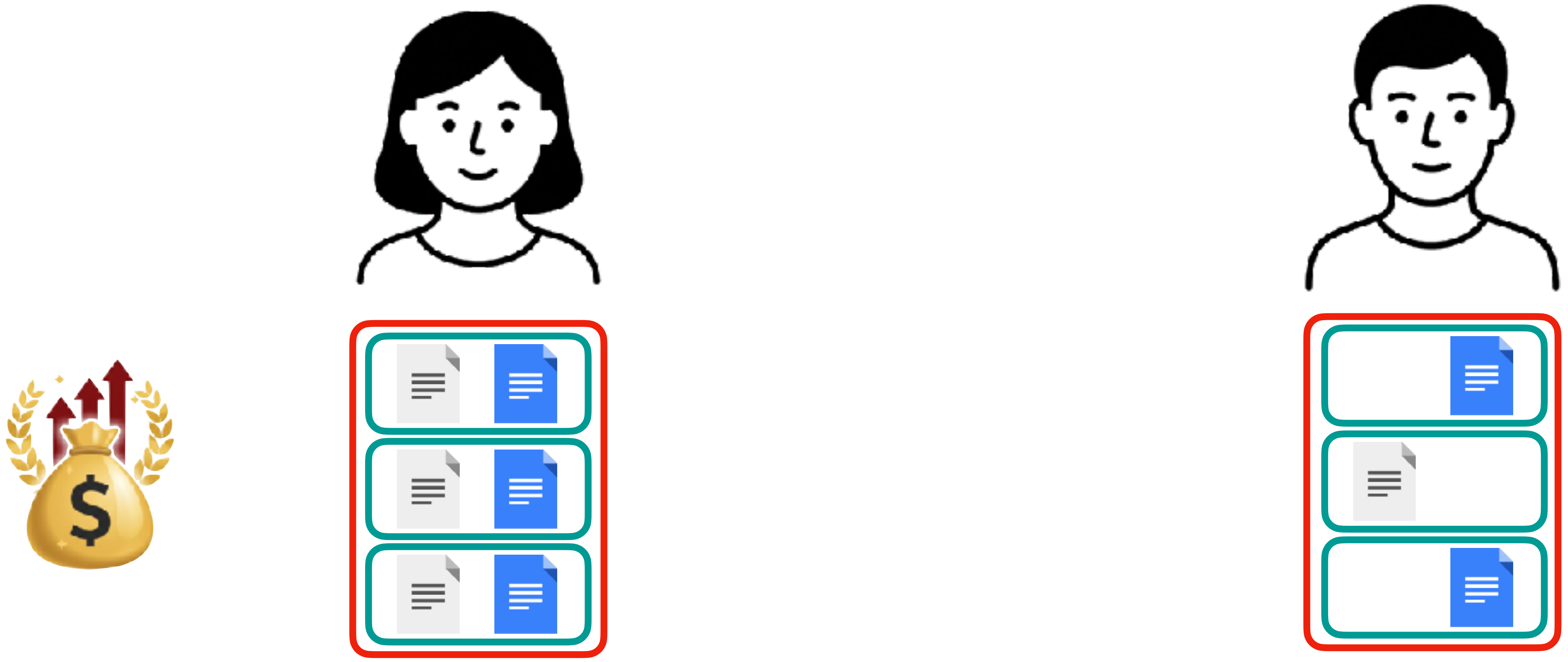
Objectif : construire un grand nombre de OT à faible coût à partir d'un petit nombre de OT coûteux

Extension de transferts inconscients

Objectif : construire un grand nombre de OT à faible coût à partir d'un petit nombre de OT coûteux

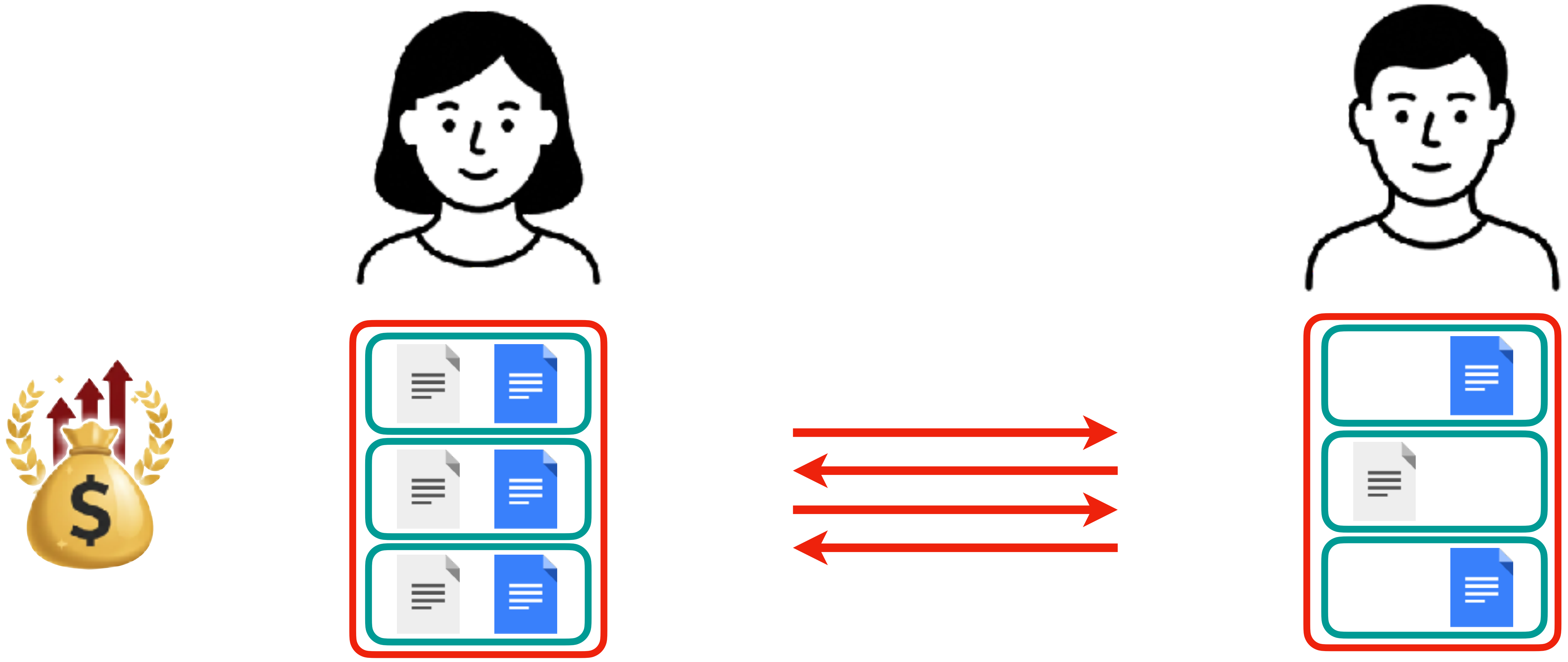
Extension de transfers inconscients

Objectif : construire un grand nombre de OT à faible coût à partir d'un petit nombre de OT coûteux



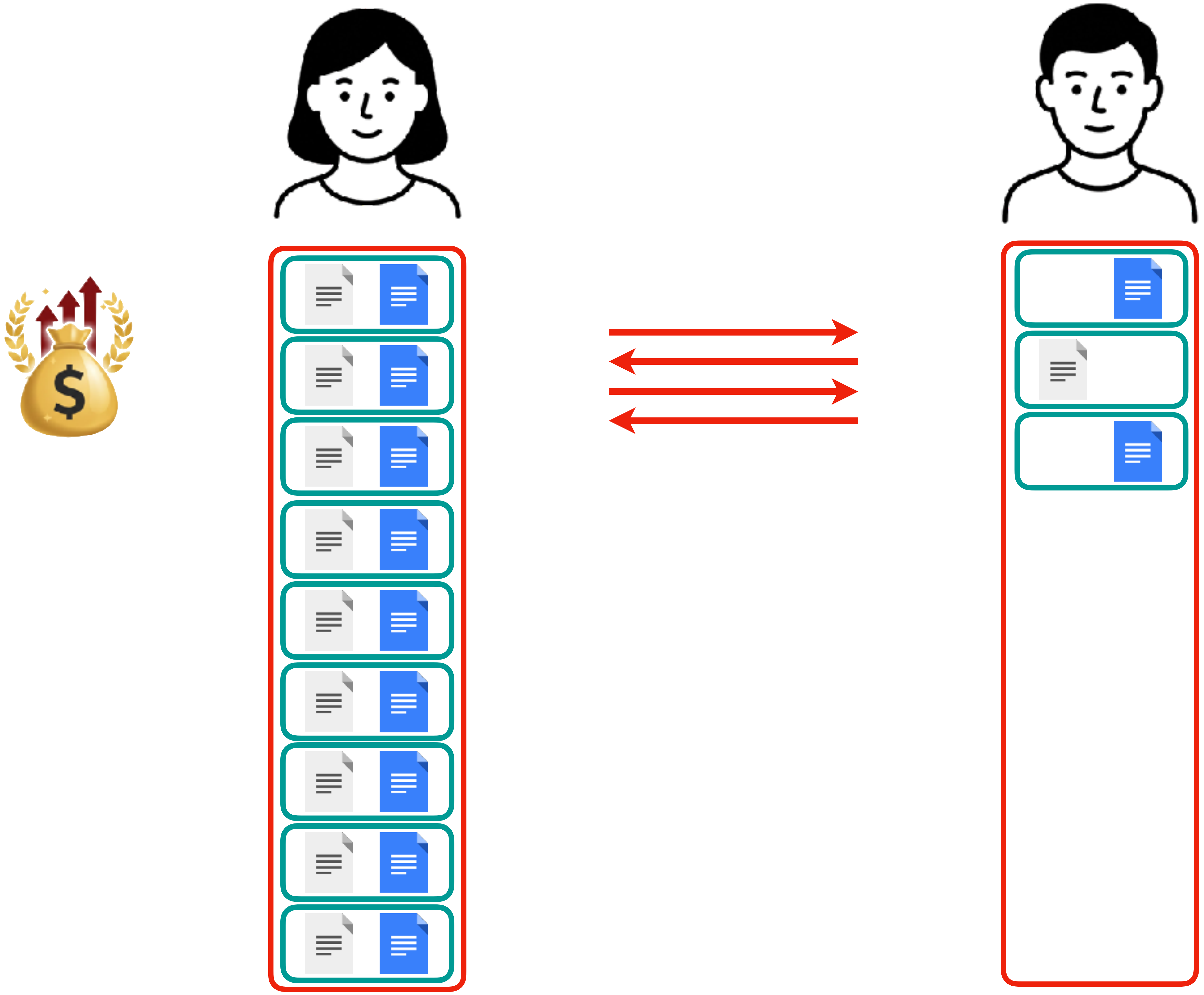
Extension de transfers inconscients

Objectif : construire un grand nombre de OT à faible coût à partir d'un petit nombre de OT coûteux



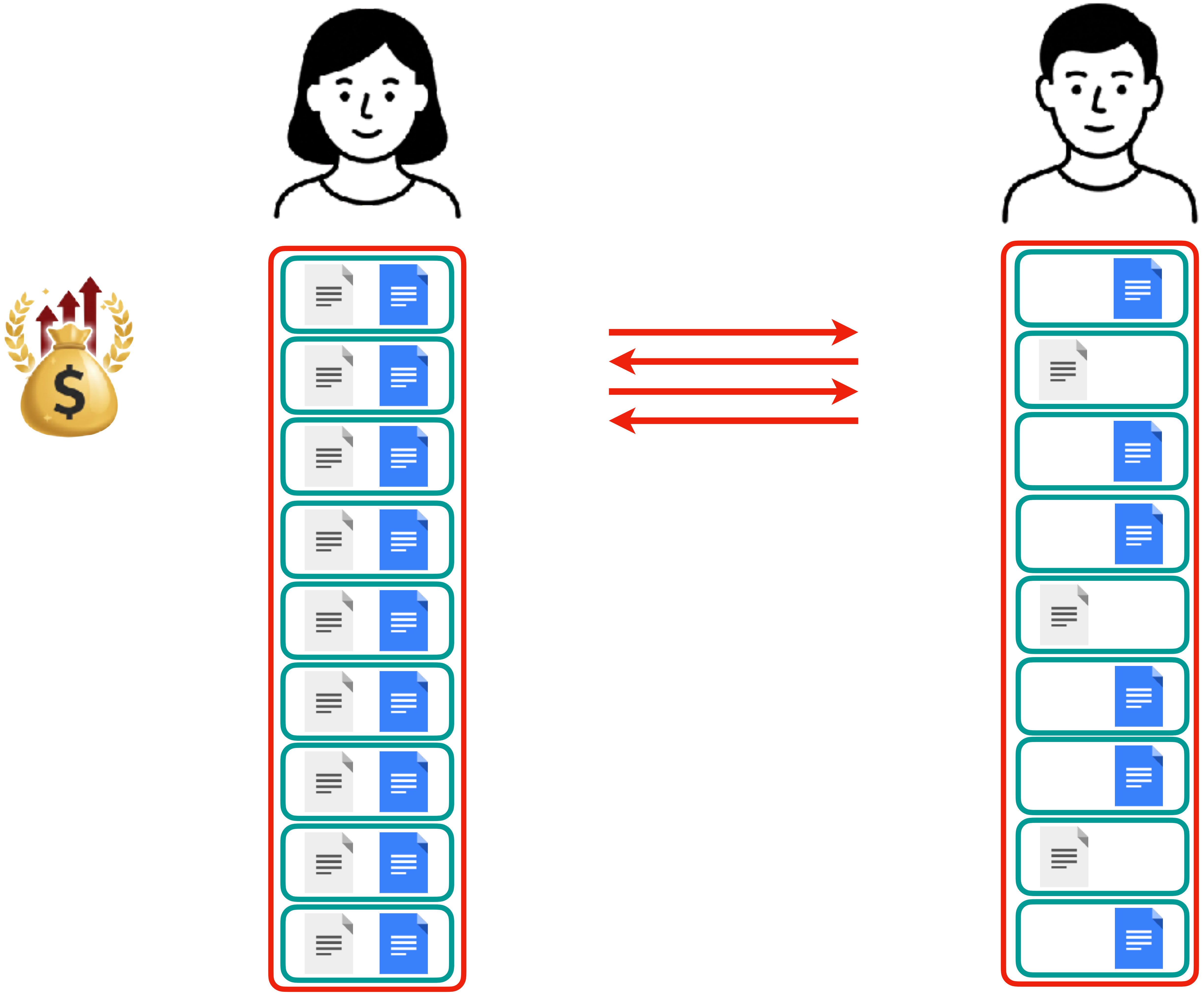
Extension de transferts inconscients

Objectif : construire un grand nombre de OT à faible coût à partir d'un petit nombre de OT coûteux



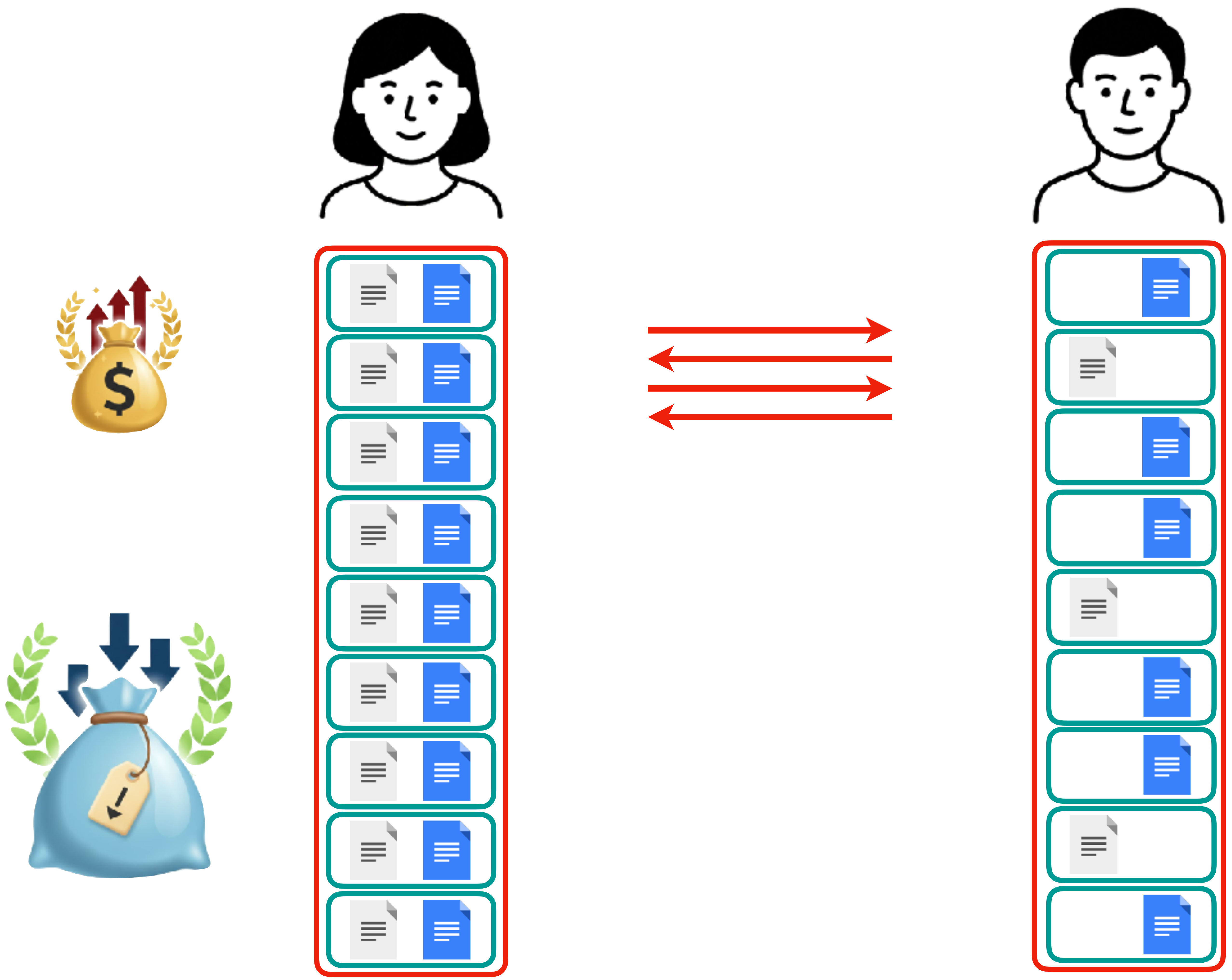
Extension de transferts inconscients

Objectif : construire un grand nombre de OT à faible coût à partir d'un petit nombre de OT coûteux



Extension de transferts inconscients

Objectif : construire un grand nombre de OT à faible coût à partir d'un petit nombre de OT coûteux

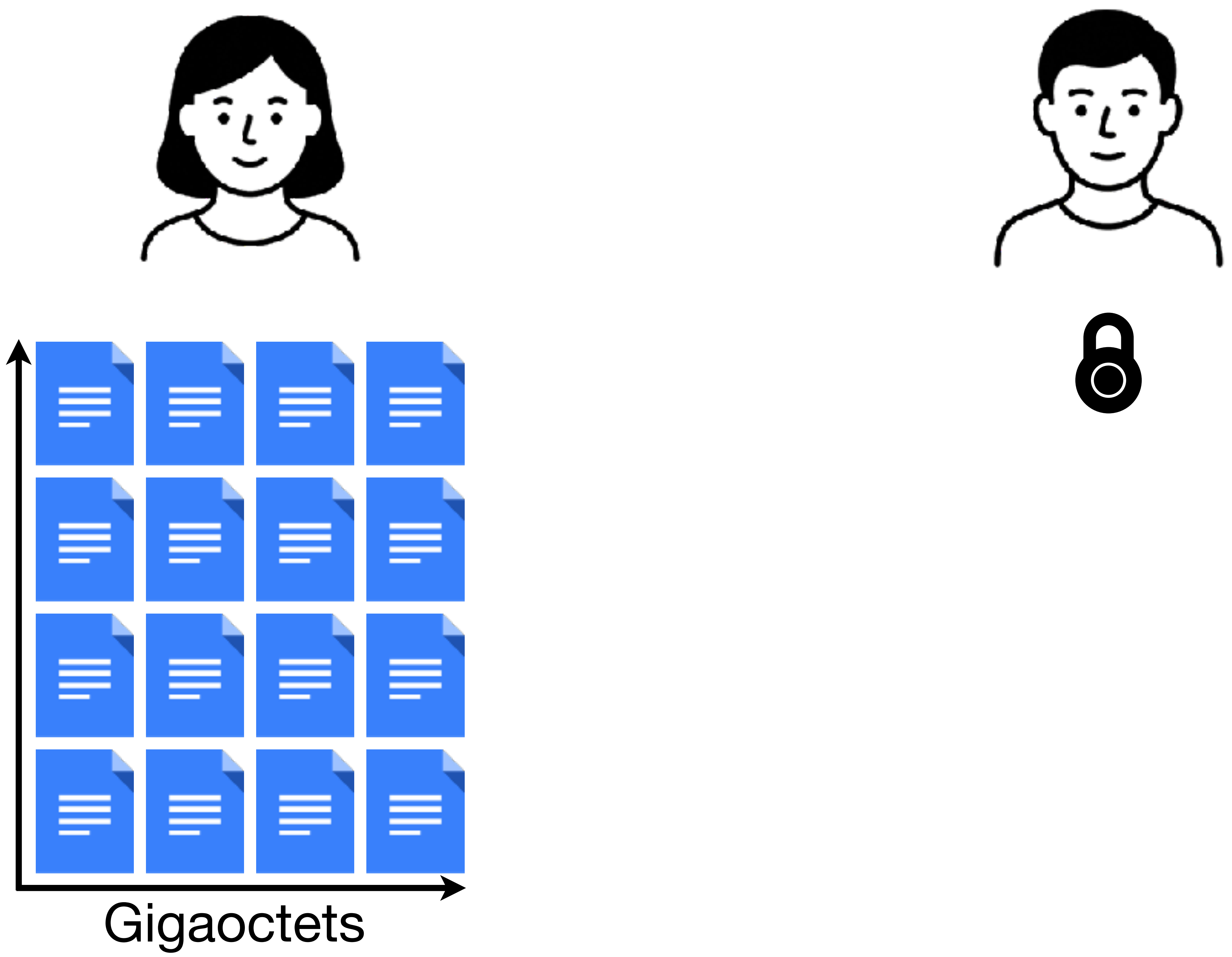


Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

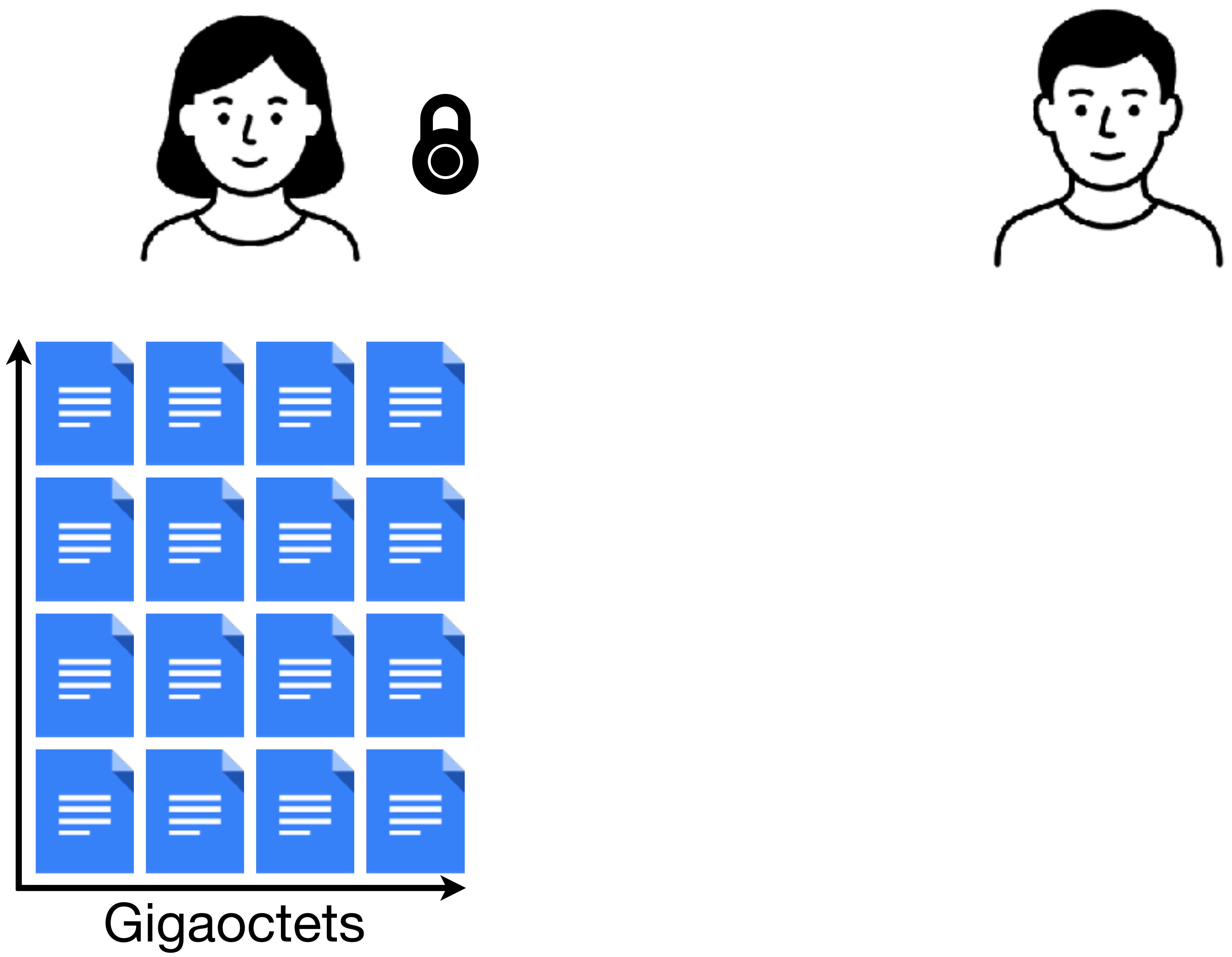
Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique



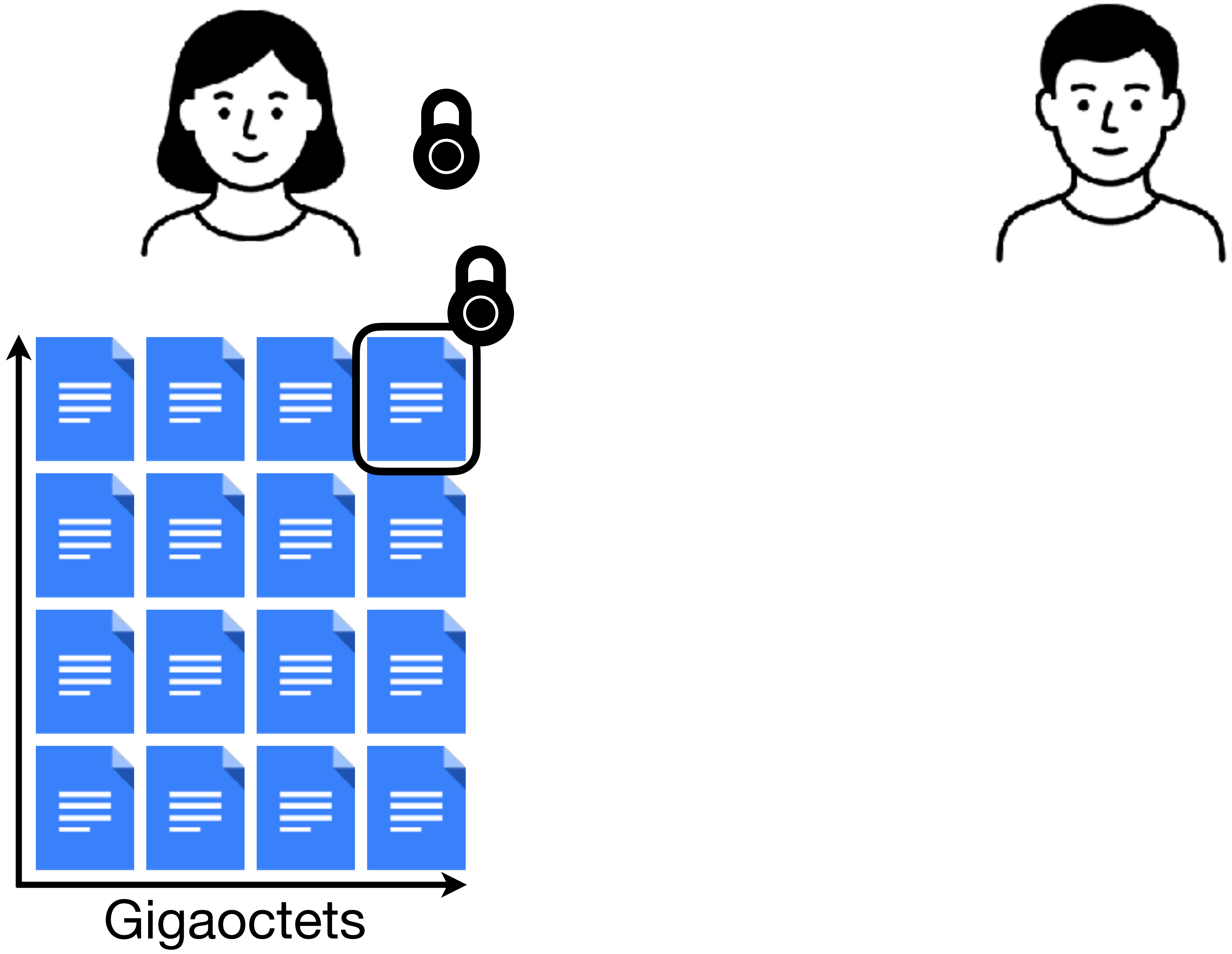
Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique



Interlude I : chiffrement hybride

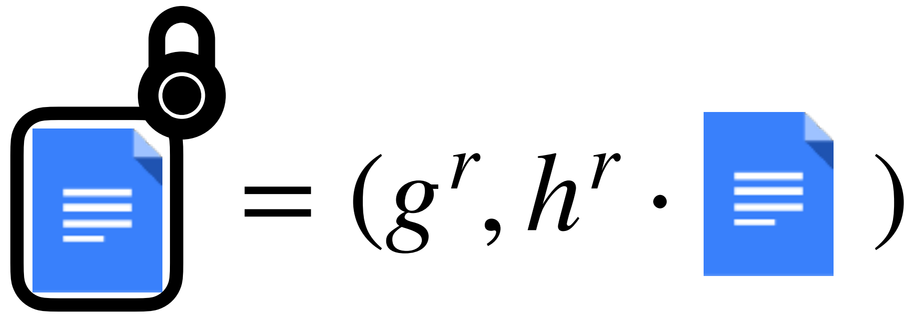
Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

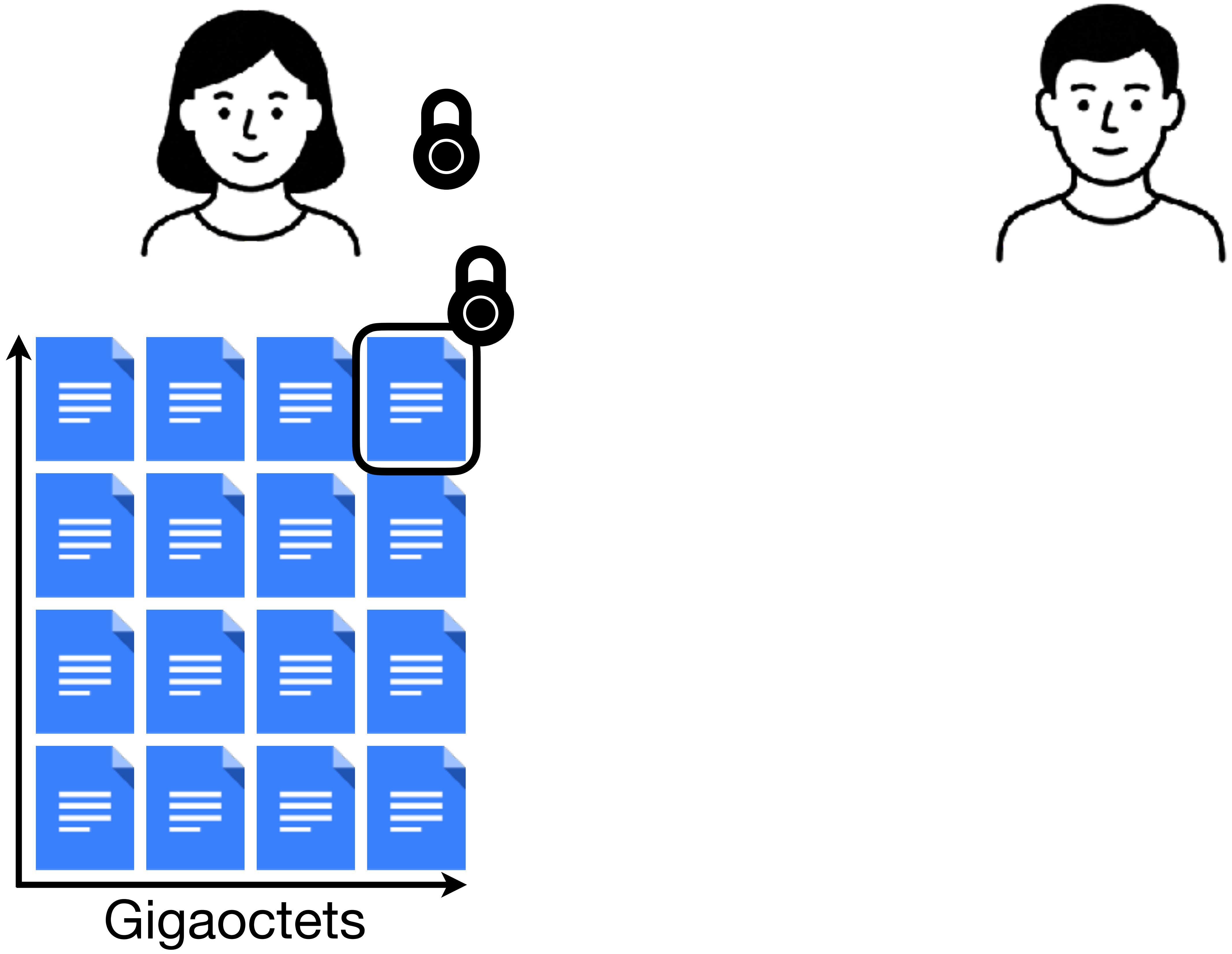


Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

Chiffrement ElGamal :

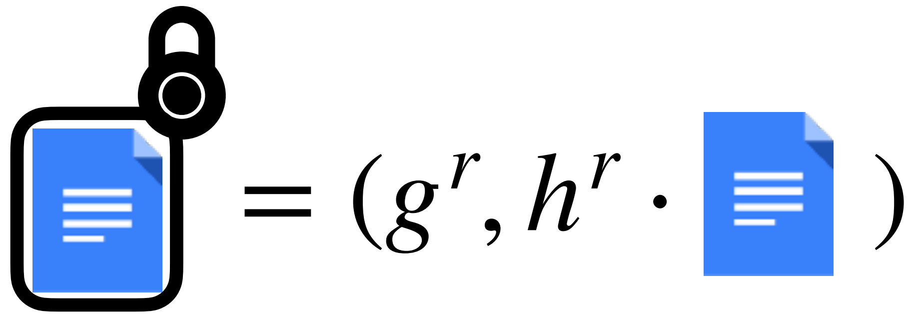


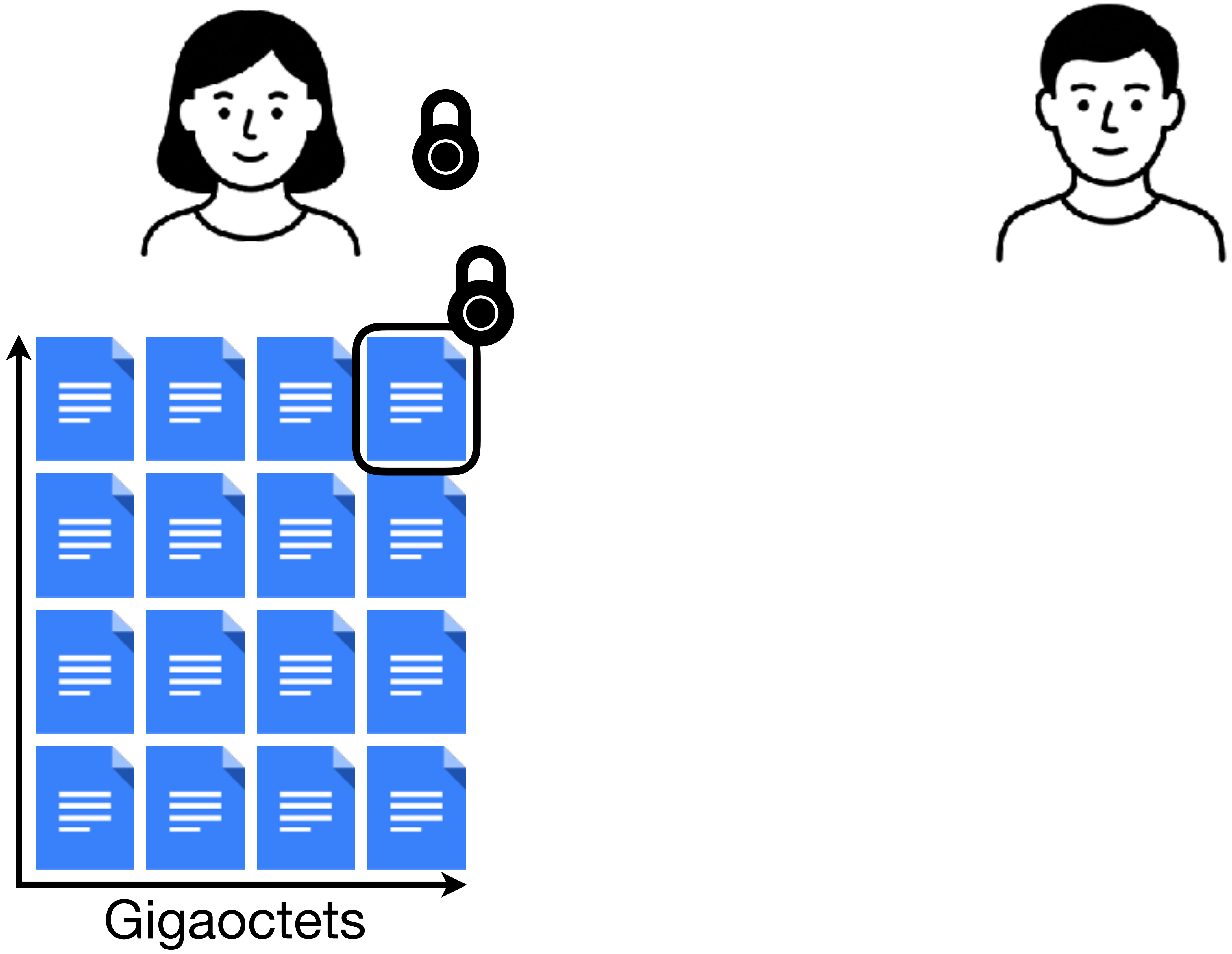


Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

Chiffrement ElGamal :



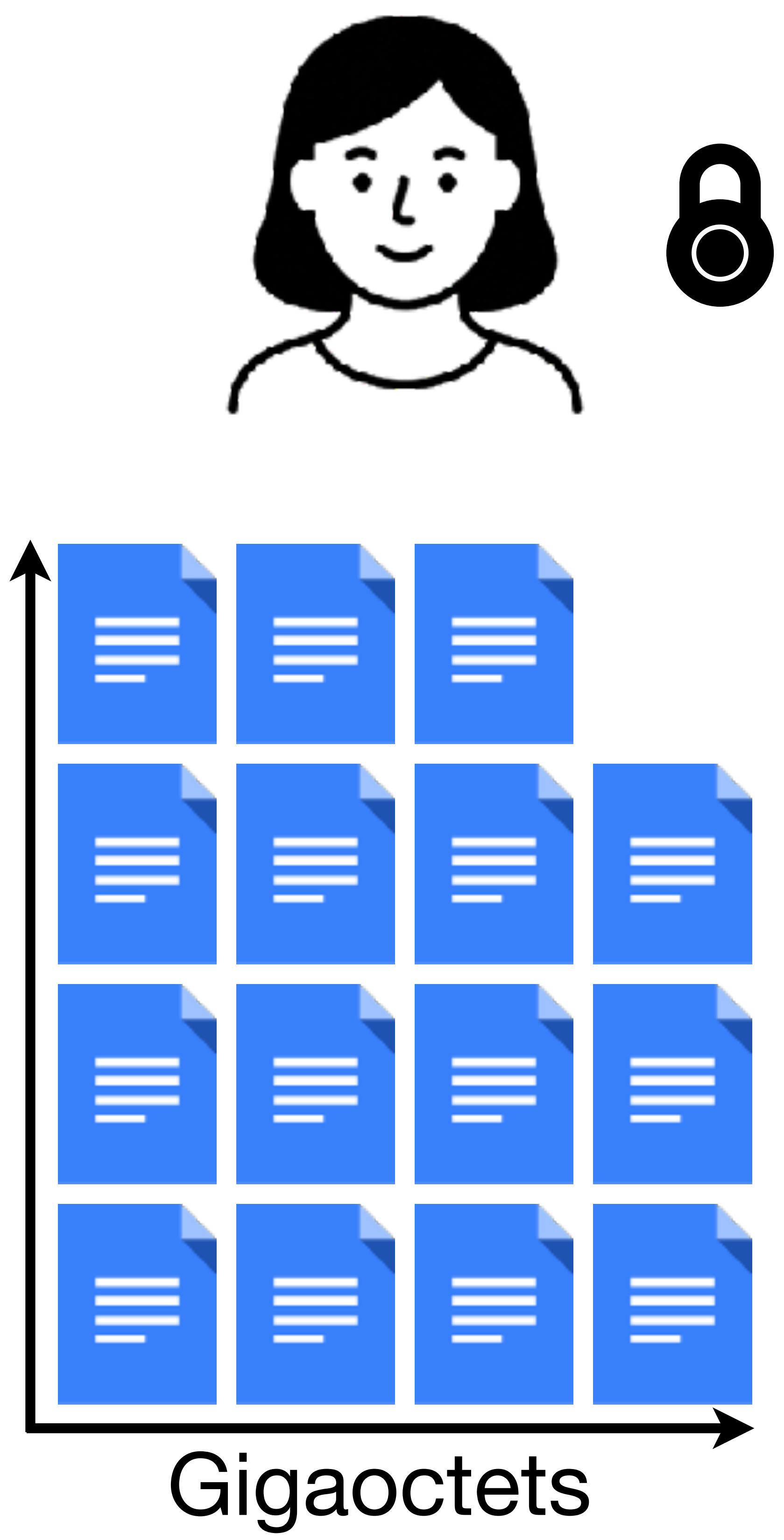


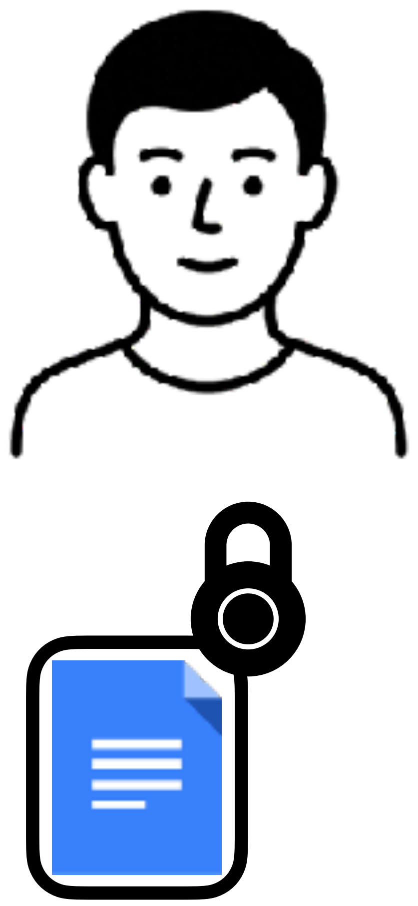
Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d’un petit nombre d’invocations d’un chiffrement à clé publique

Chiffrement ElGamal :

 $= (g^r, h^r \cdot$  $)$

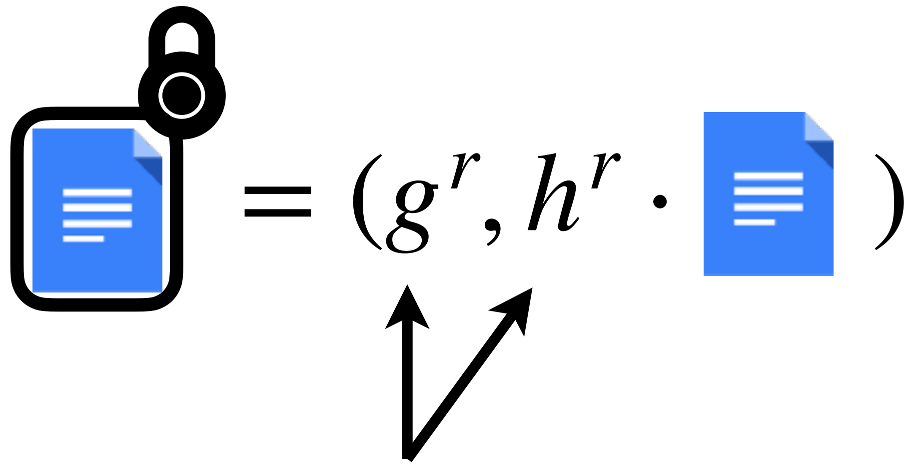




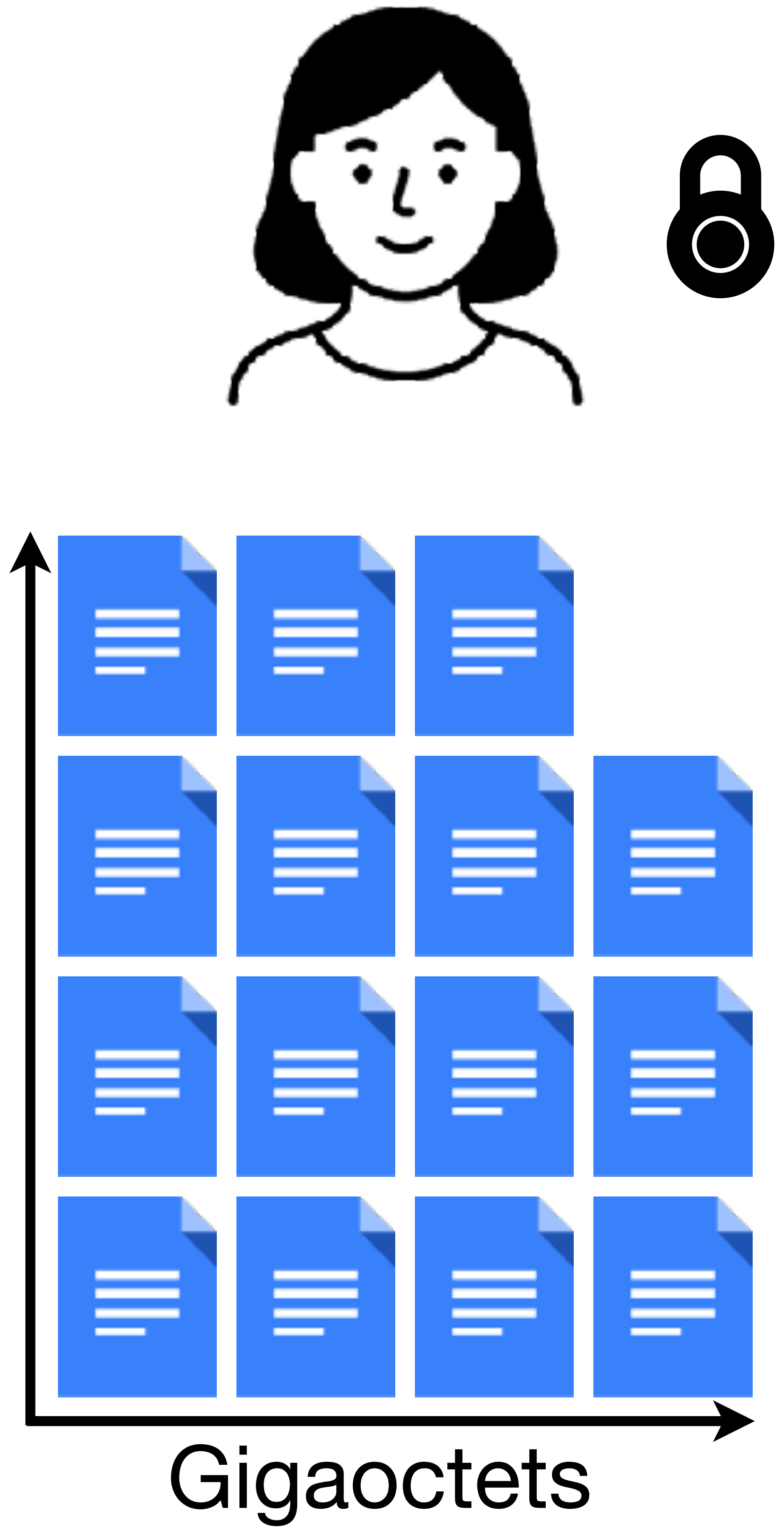
Interlude I : chiffrement hybride

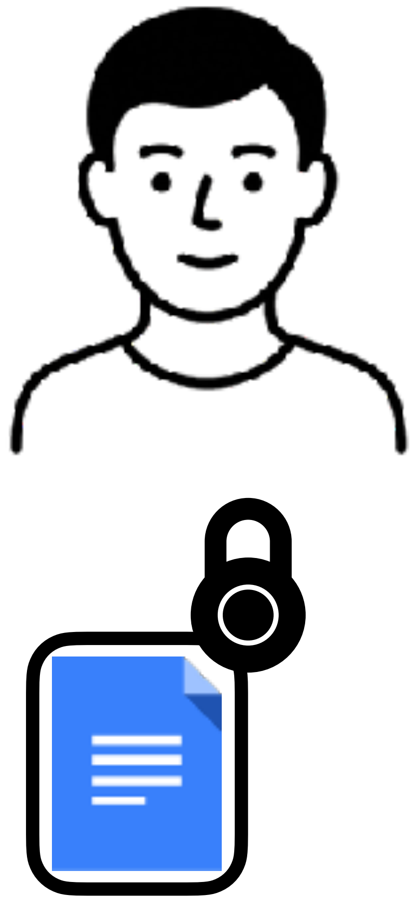
Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

Chiffrement ElGamal :



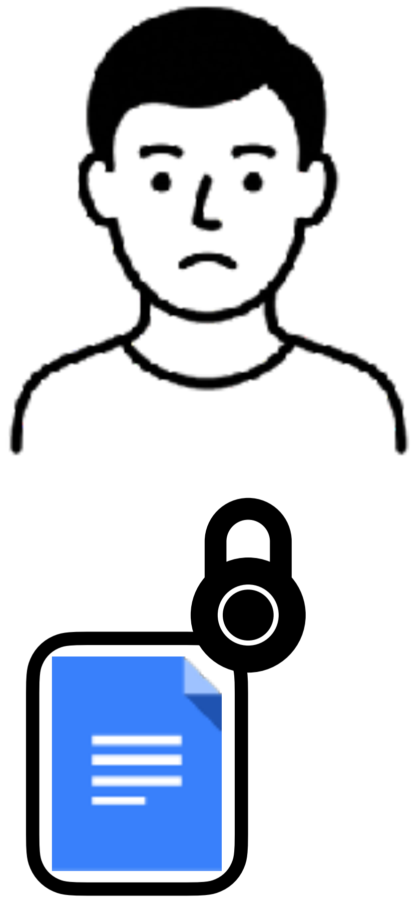
Deux exponentiations
(~ quelques dizaines de us)





Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique



Chiffrement ElGamal :

 $= (g^r, h^r \cdot$  $)$

Deux exponentiations
(~ quelques dizaines de us)

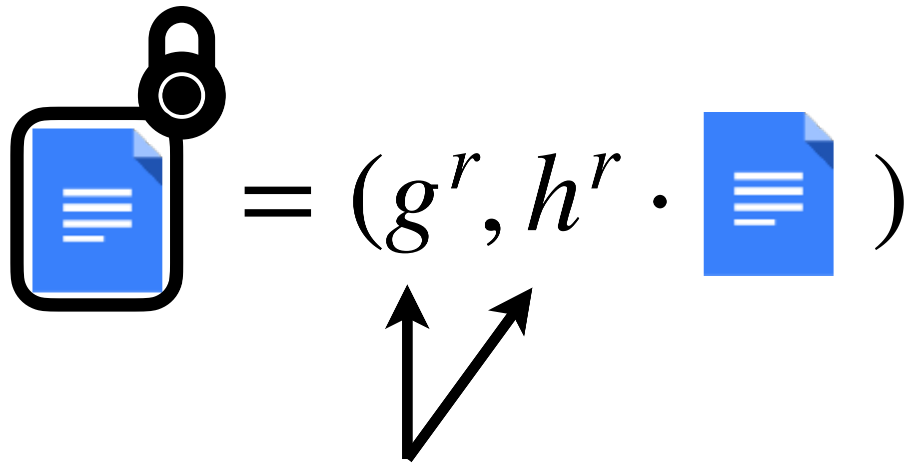
3.5 mois

Gigaoctets

Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

Chiffrement ElGamal :



Deux exponentiations
(~ quelques dizaines de us)

Générateur pseudo-aléatoire :

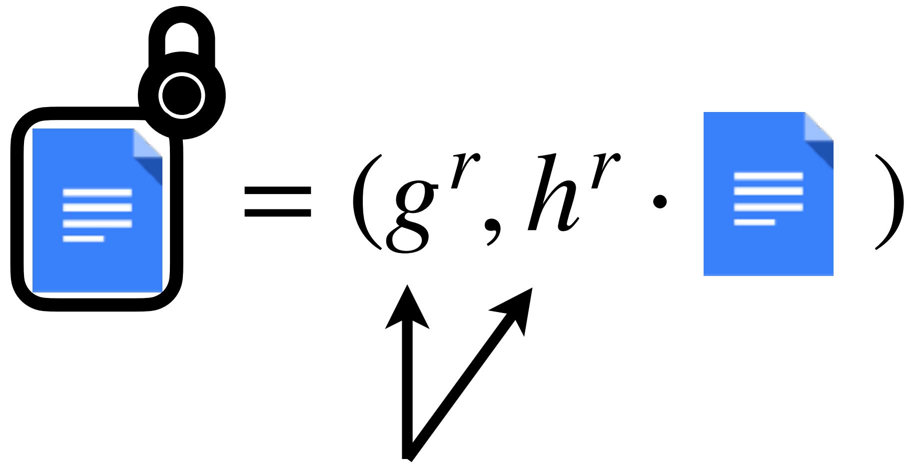
Un générateur $G : \{0,1\}^n \to \{0,1\}^*$ prend en entrée une « graine » $x \in \{0,1\}^n$ et produit une sortie $y = G(x)$ *indistinguable d'une chaîne aléatoire*

(Typiquement, $n = 128$)

Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

Chiffrement ElGamal :



Deux exponentiations
(~ quelques dizaines de us)

Générateur pseudo-aléatoire :

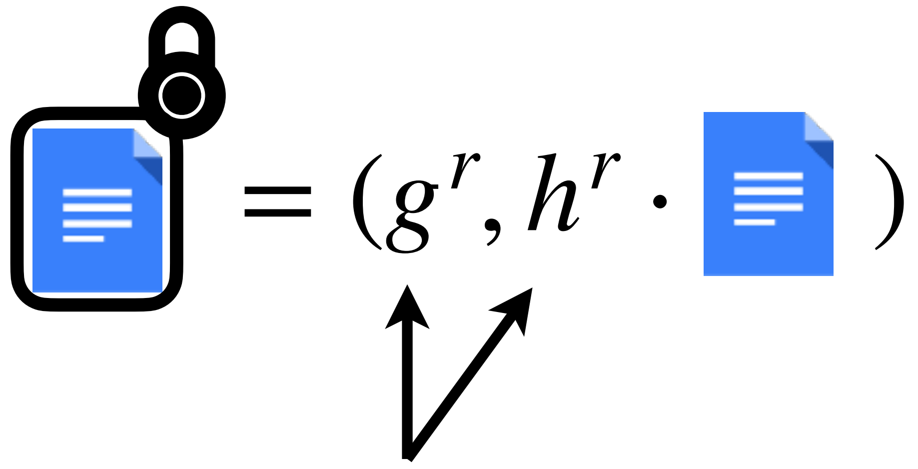
Un générateur $G : \{0,1\}^n \to \{0,1\}^*$ prend en entrée une « graine » $x \in \{0,1\}^n$ et produit une sortie $y = G(x)$ *indistinguable d'une chaîne aléatoire*

(Typiquement, $n = 128$)

Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

Chiffrement ElGamal :



Deux exponentiations
(~ quelques dizaines de us)

Prend  au hasard

Générateur pseudo-aléatoire :

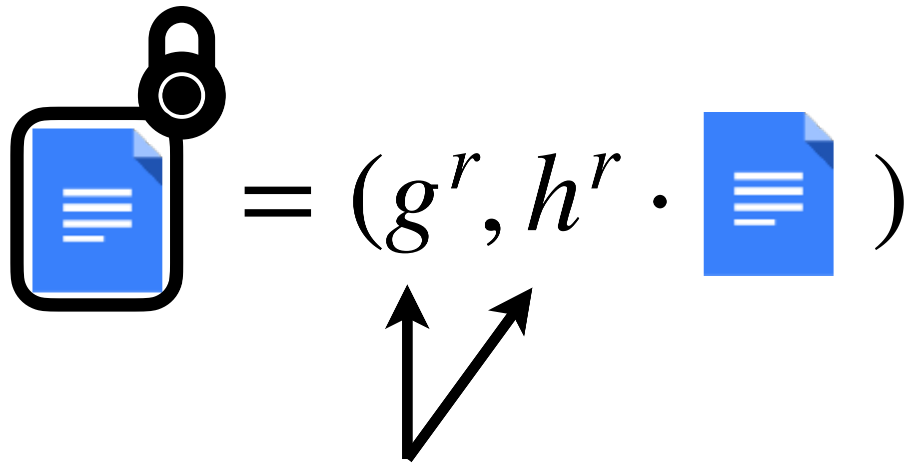
Un générateur $G : \{0,1\}^n \to \{0,1\}^*$ prend en entrée une « graine » $x \in \{0,1\}^n$ et produit une sortie $y = G(x)$ *indistinguable d'une chaîne aléatoire*

(Typiquement, $n = 128$)

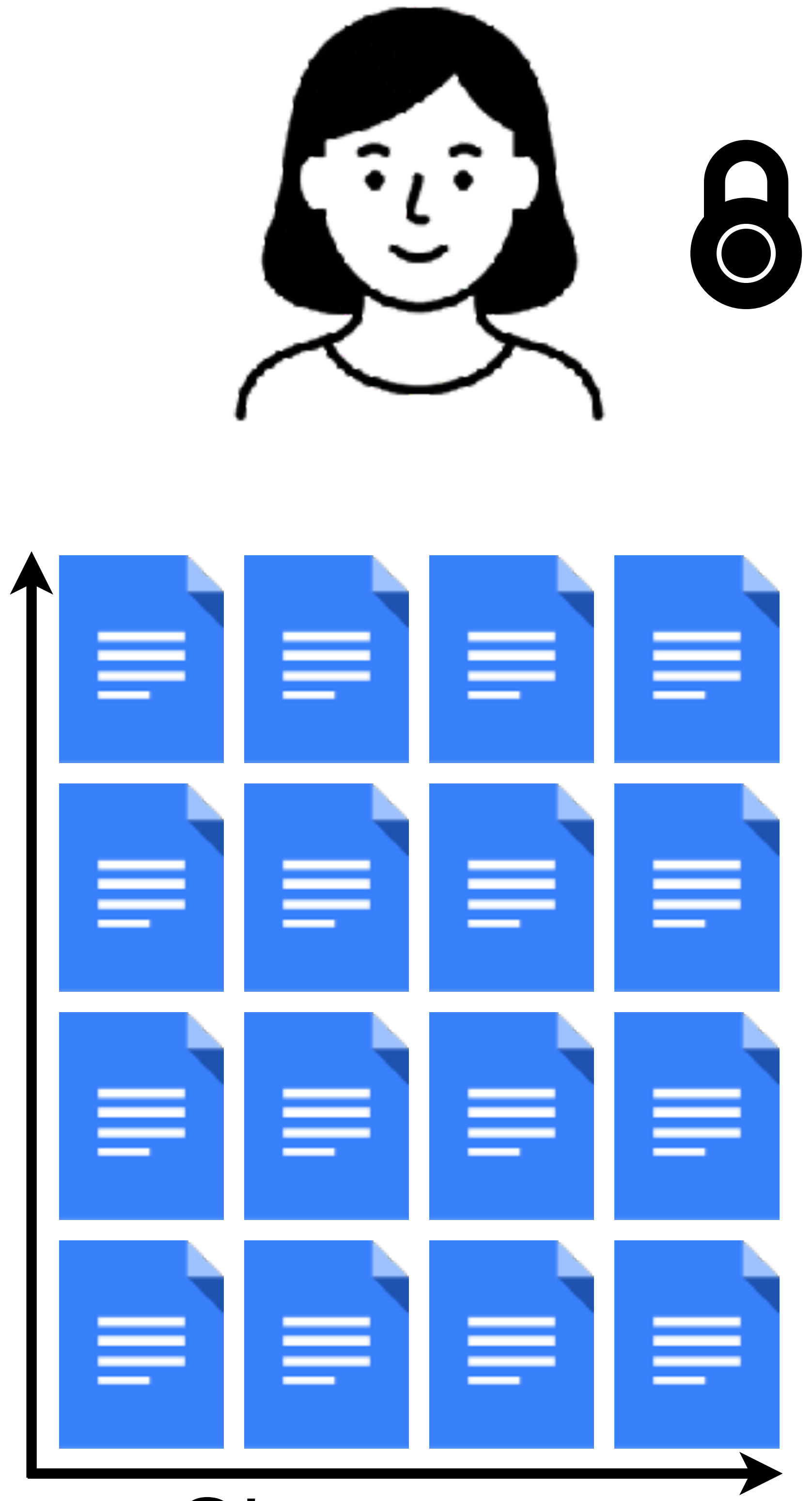
Interlude I : chiffrement hybride

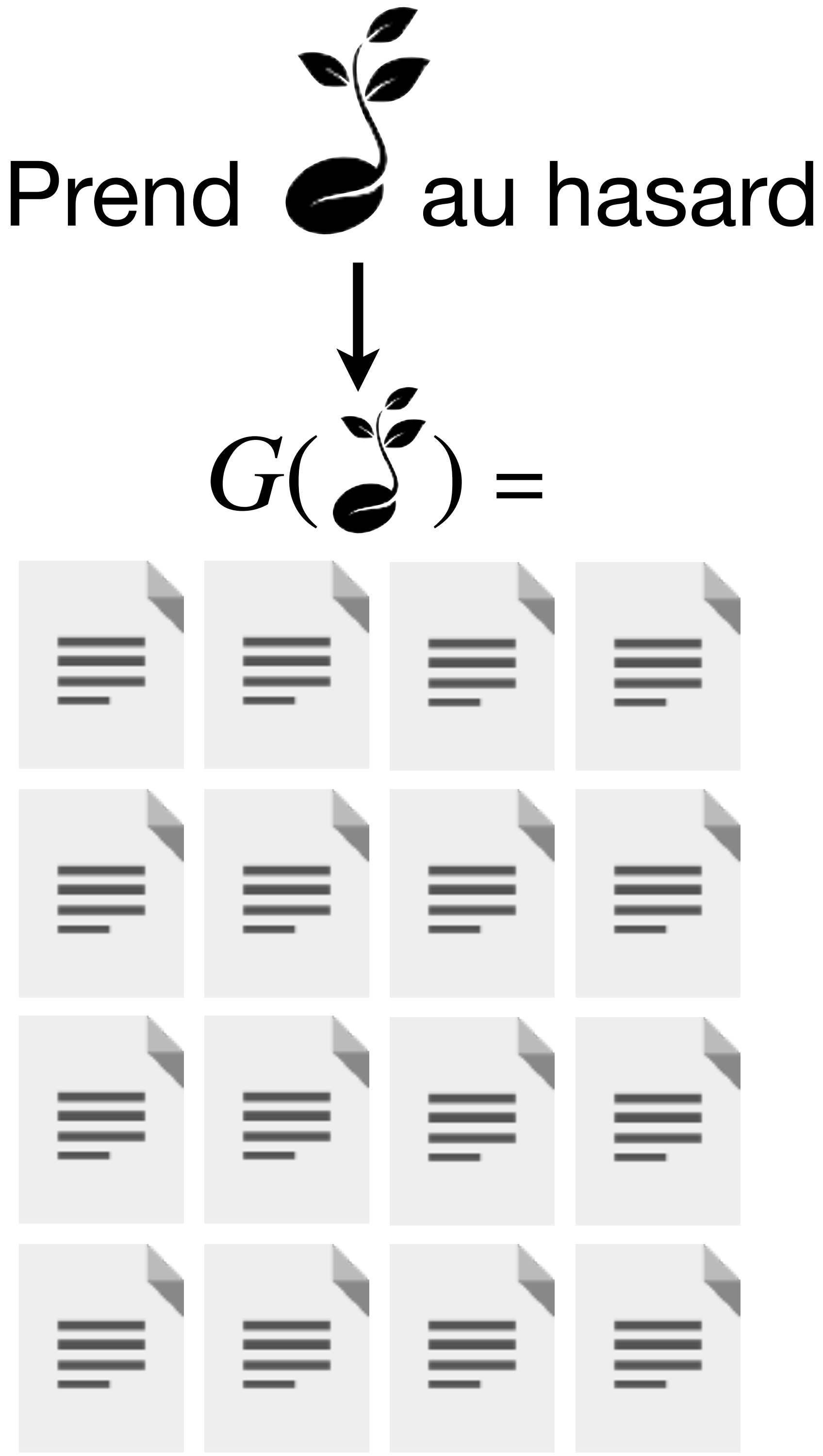
Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

Chiffrement ElGamal :



Deux exponentiations
(~ quelques dizaines de us)





Générateur pseudo-aléatoire :

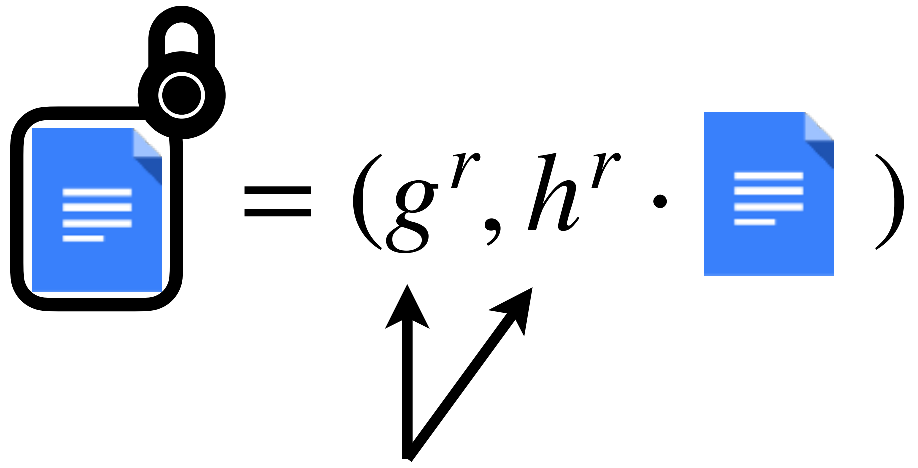
Un générateur $G : \{0,1\}^n \rightarrow \{0,1\}^*$ prend en entrée une « graine » $x \in \{0,1\}^n$ et produit une sortie $y = G(x)$ *indistinguable d'une chaîne aléatoire*

(Typiquement, $n = 128$)

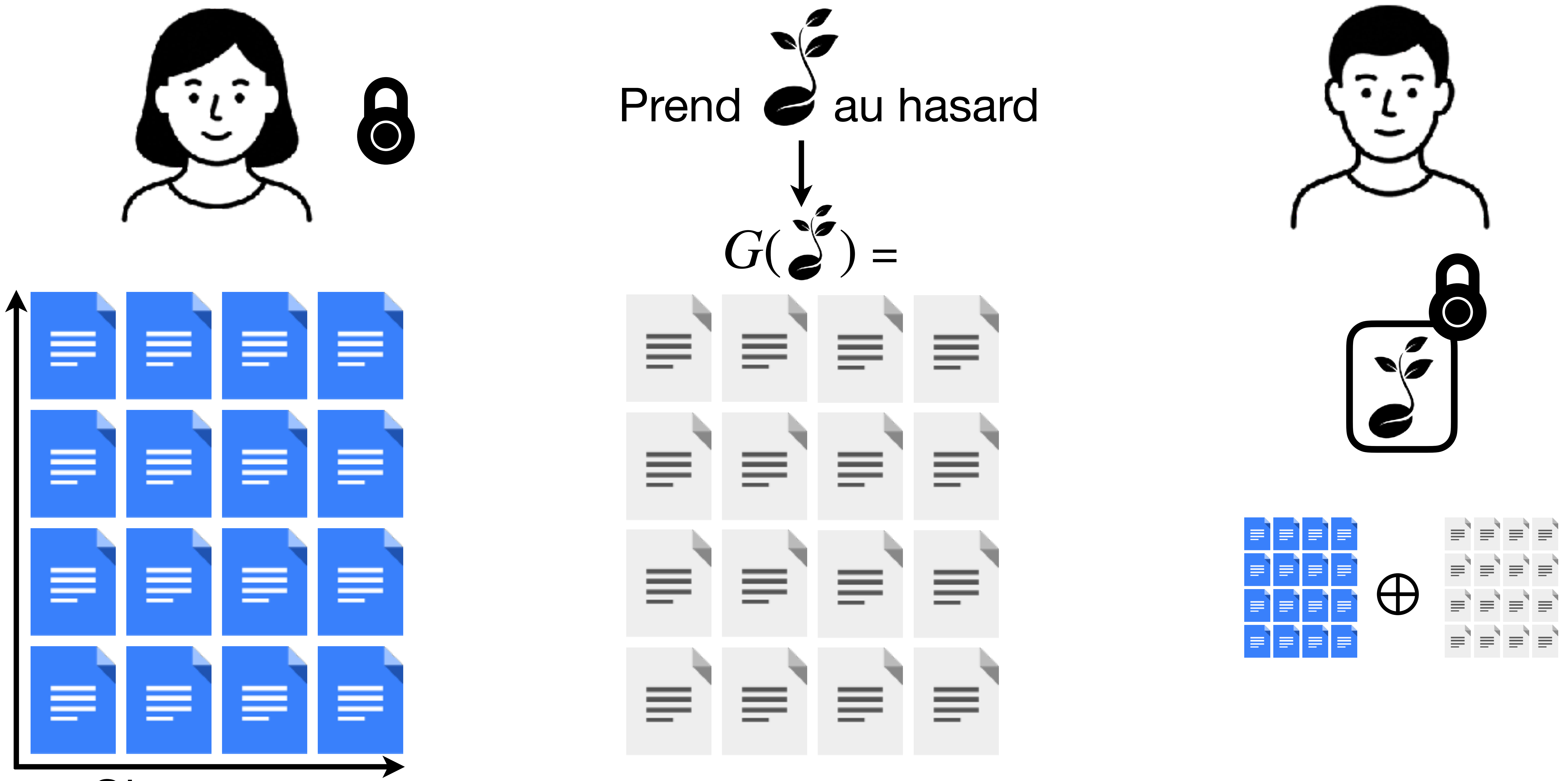
Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

Chiffrement ElGamal :



Deux exponentiations
(~ quelques dizaines de us)



Gigaoctets

Générateur pseudo-aléatoire :

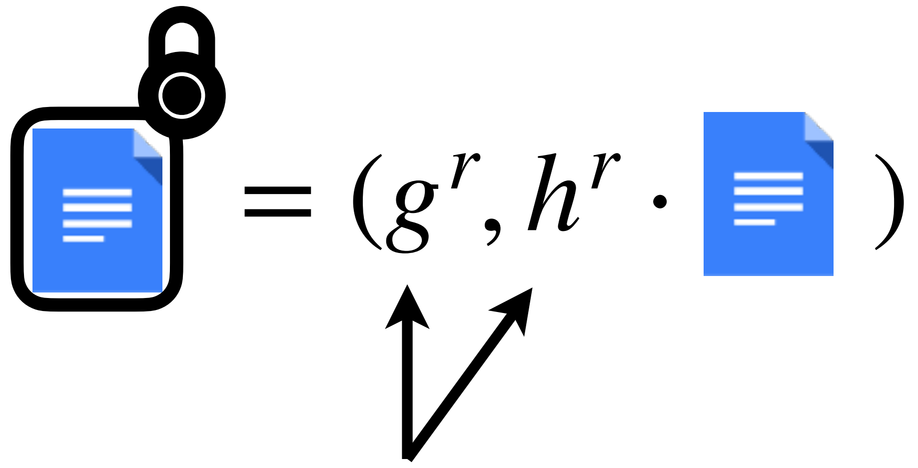
Un générateur $G : \{0,1\}^n \rightarrow \{0,1\}^*$ prend en entrée une « graine » $x \in \{0,1\}^n$ et produit une sortie $y = G(x)$ *indistinguable d'une chaîne aléatoire*

(Typiquement, $n = 128$)

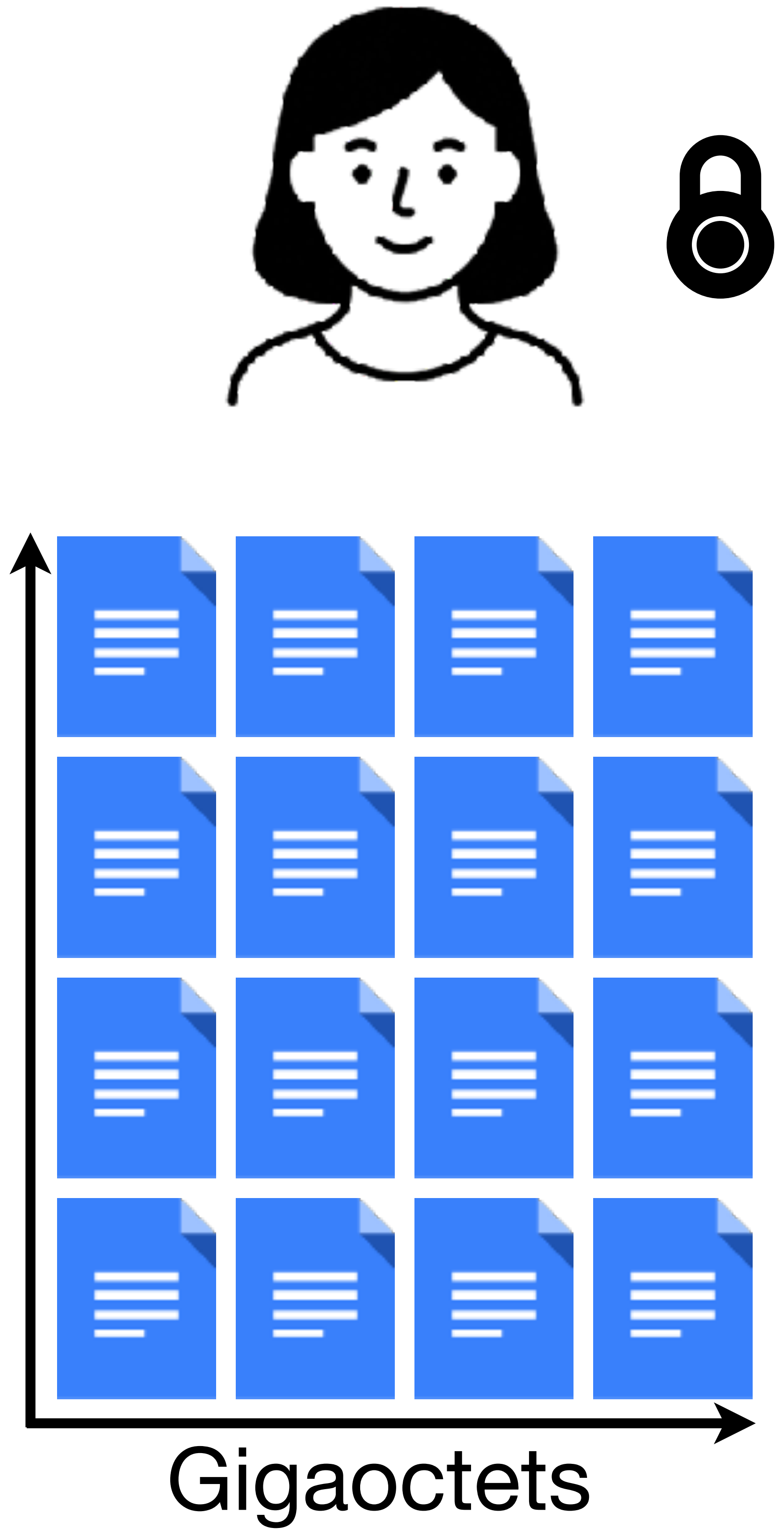
Interlude I : chiffrement hybride

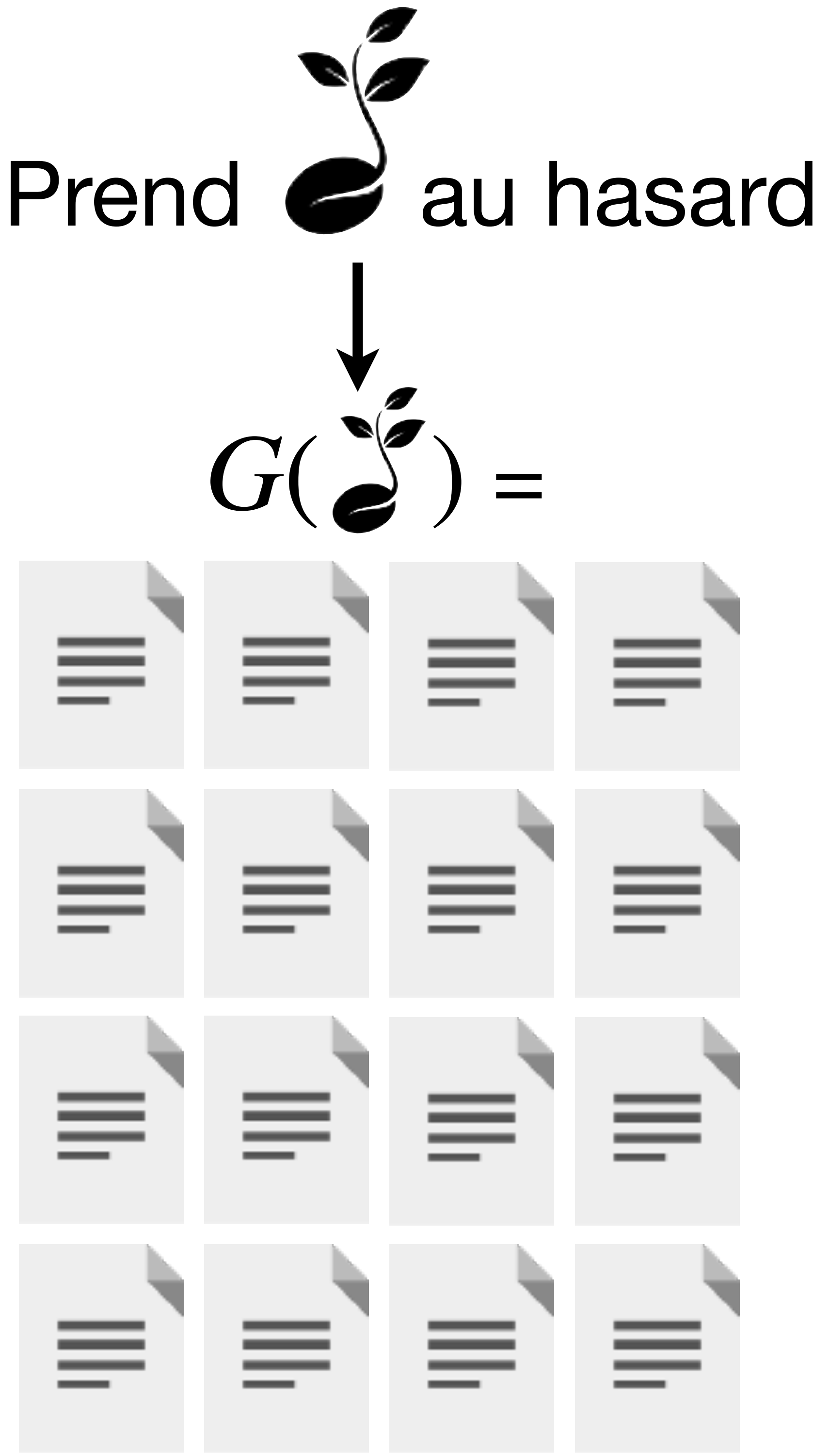
Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

Chiffrement ElGamal :



Deux exponentiations
(~ quelques dizaines de us)





Générateur pseudo-aléatoire :

Un générateur $G : \{0,1\}^n \to \{0,1\}^*$ prend en entrée une « graine » $x \in \{0,1\}^n$ et produit une sortie $y = G(x)$ *indistinguable d'une chaîne aléatoire*

(Typiquement, $n = 128$)

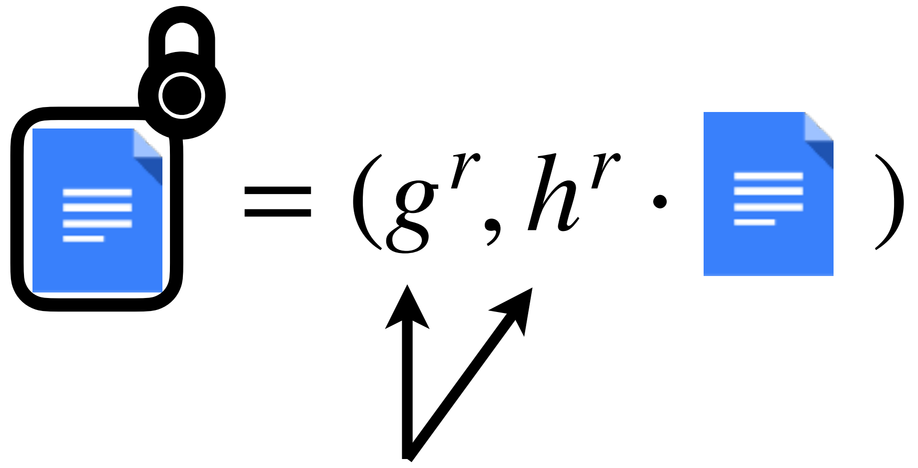
: avec AES-NI, 1.3 cycles/octet
=> 1.85 Go/s (CPU 2.4GHz)

: |données| + 64 octets

Interlude I : chiffrement hybride

Objectif : chiffrer une grande quantité de données à partir d'un petit nombre d'invocations d'un chiffrement à clé publique

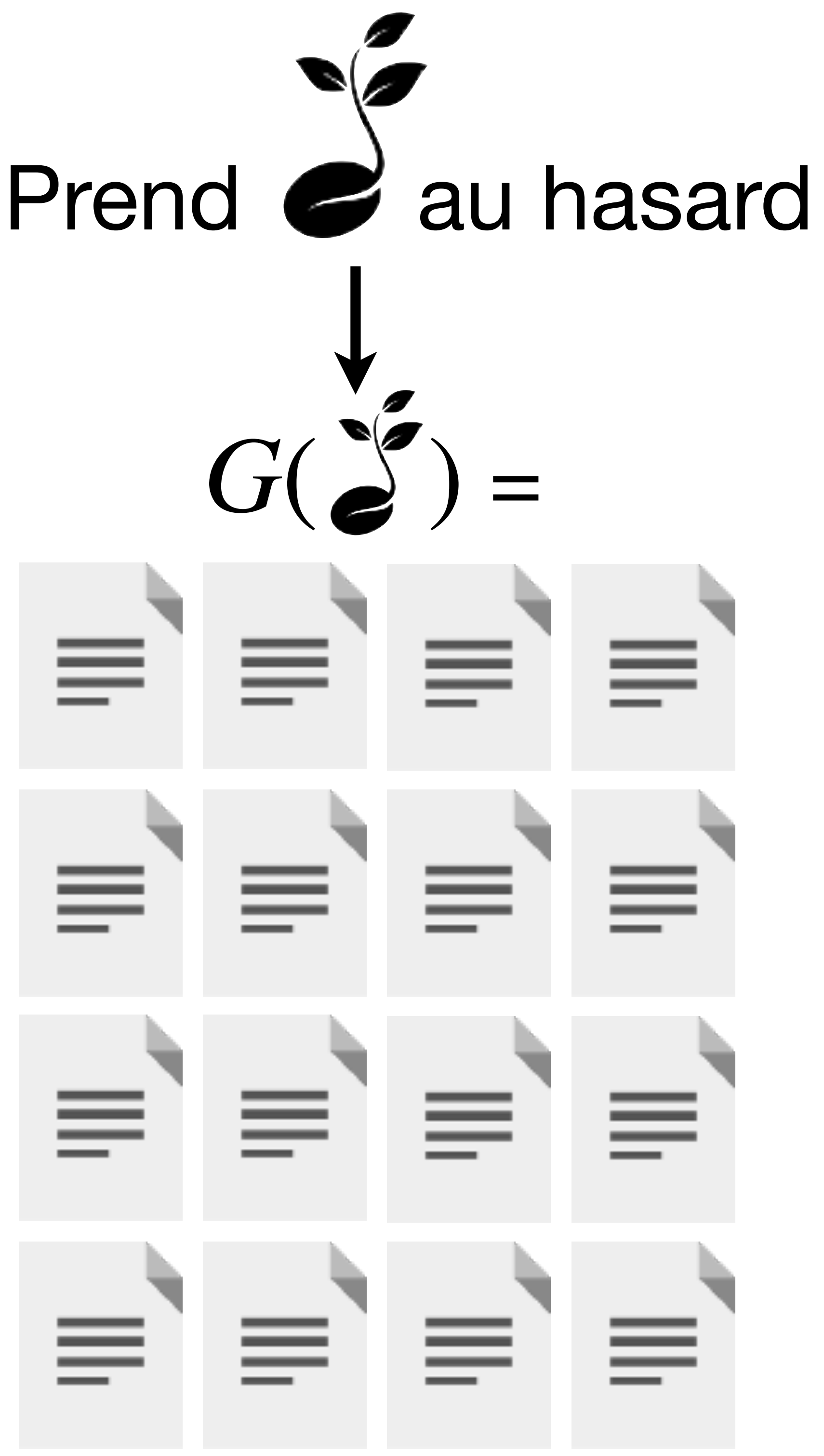
Chiffrement ElGamal :



Deux exponentiations
(~ quelques dizaines de us)

0.6 secondes

Gigaoctets



Générateur pseudo-aléatoire :

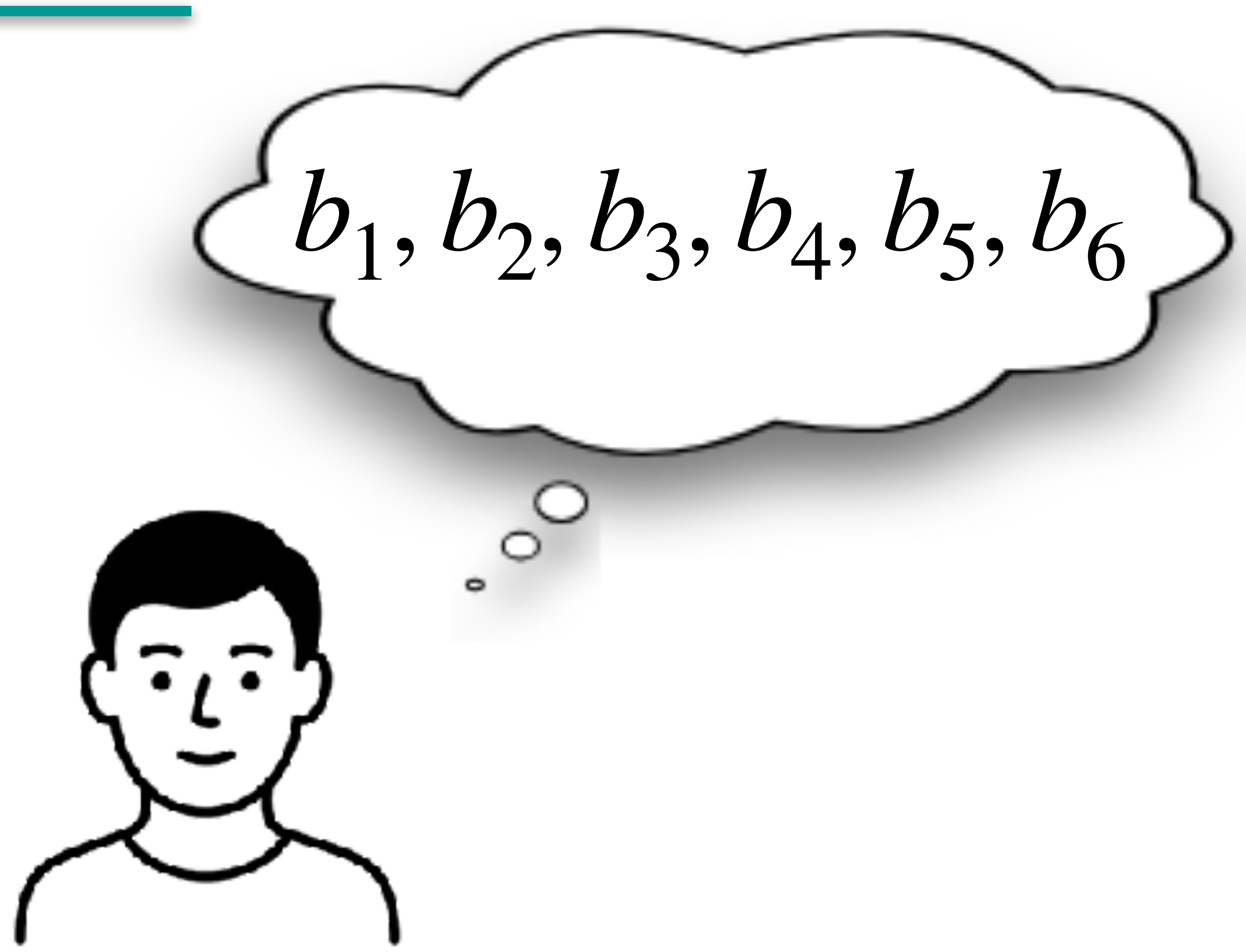
Un générateur $G : \{0,1\}^n \to \{0,1\}^*$ prend en entrée une « graine » $x \in \{0,1\}^n$ et produit une sortie $y = G(x)$ *indistinguable d'une chaîne aléatoire*

(Typiquement, $n = 128$)

: avec AES-NI, 1.3 cycles/octet
=> 1.85 Go/s (CPU 2.4GHz)

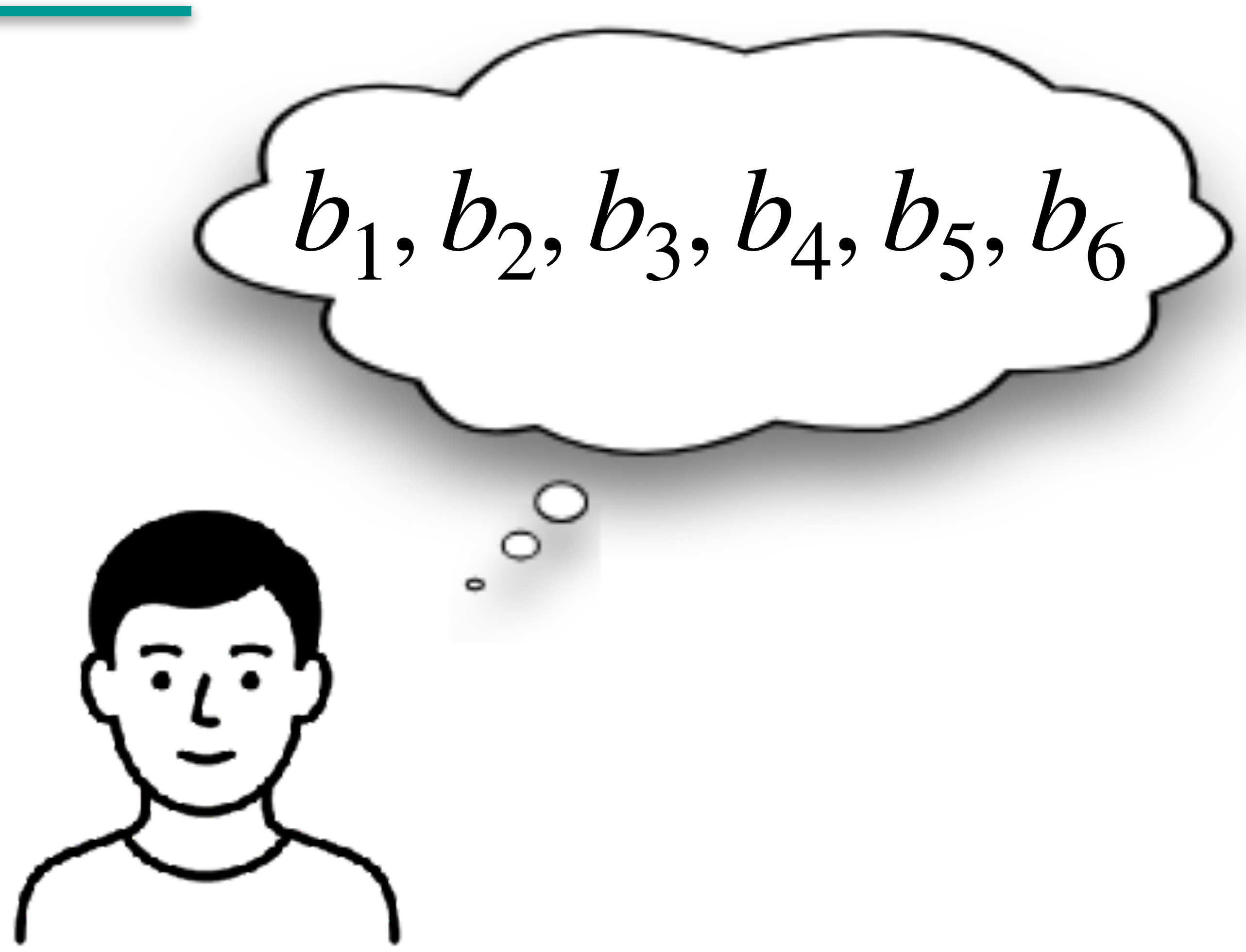
: |données| + 64 octets

Transferts Inconscients corrélés



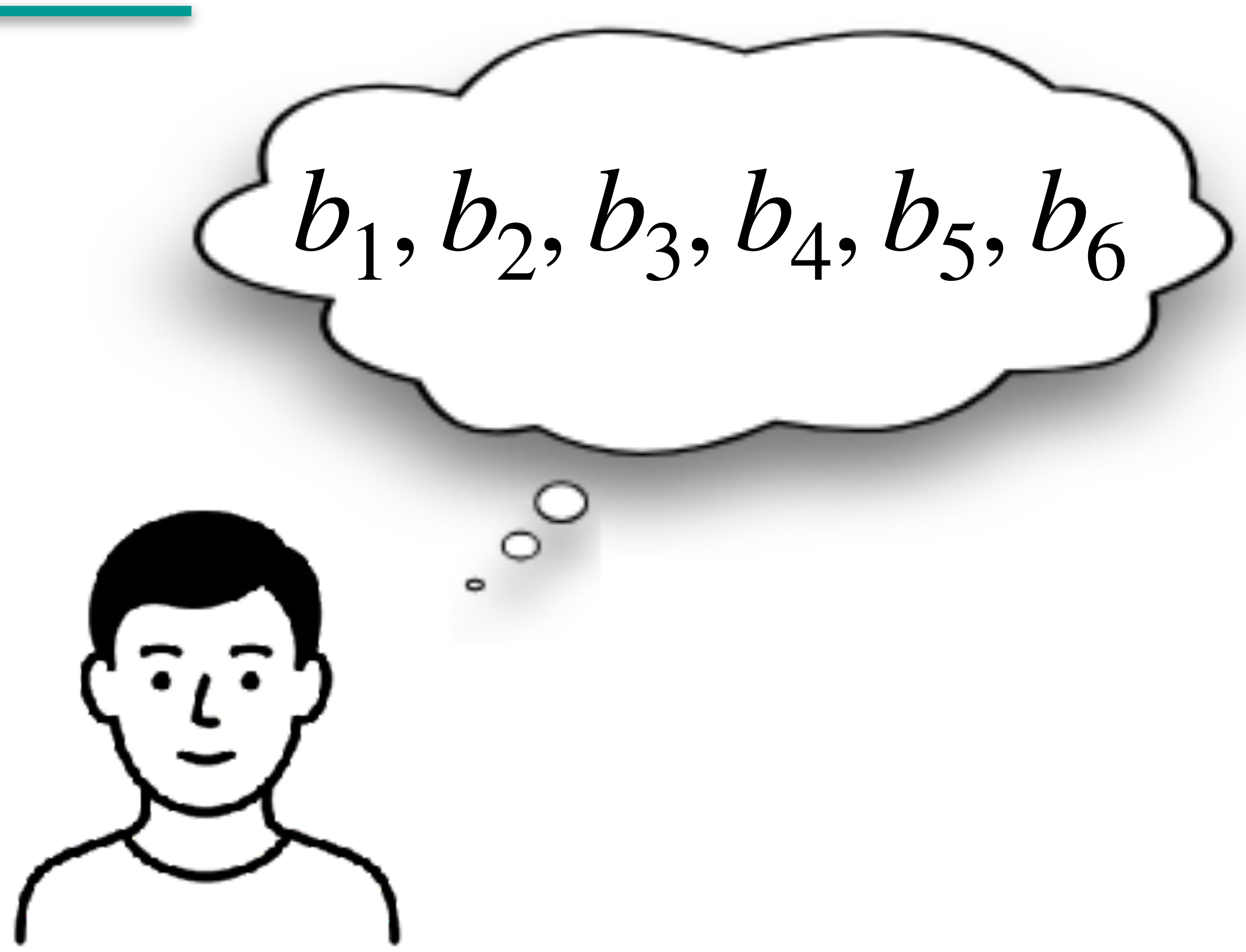
u_1	v_1
u_2	v_2
u_3	v_3
u_4	v_4
u_5	v_5
u_6	v_6

Transferts Inconscients corrélés



u_1	$u_1 + \delta_1$
u_2	$u_2 + \delta_2$
u_3	$u_3 + \delta_3$
u_4	$u_4 + \delta_4$
u_5	$u_5 + \delta_5$
u_6	$u_6 + \delta_6$

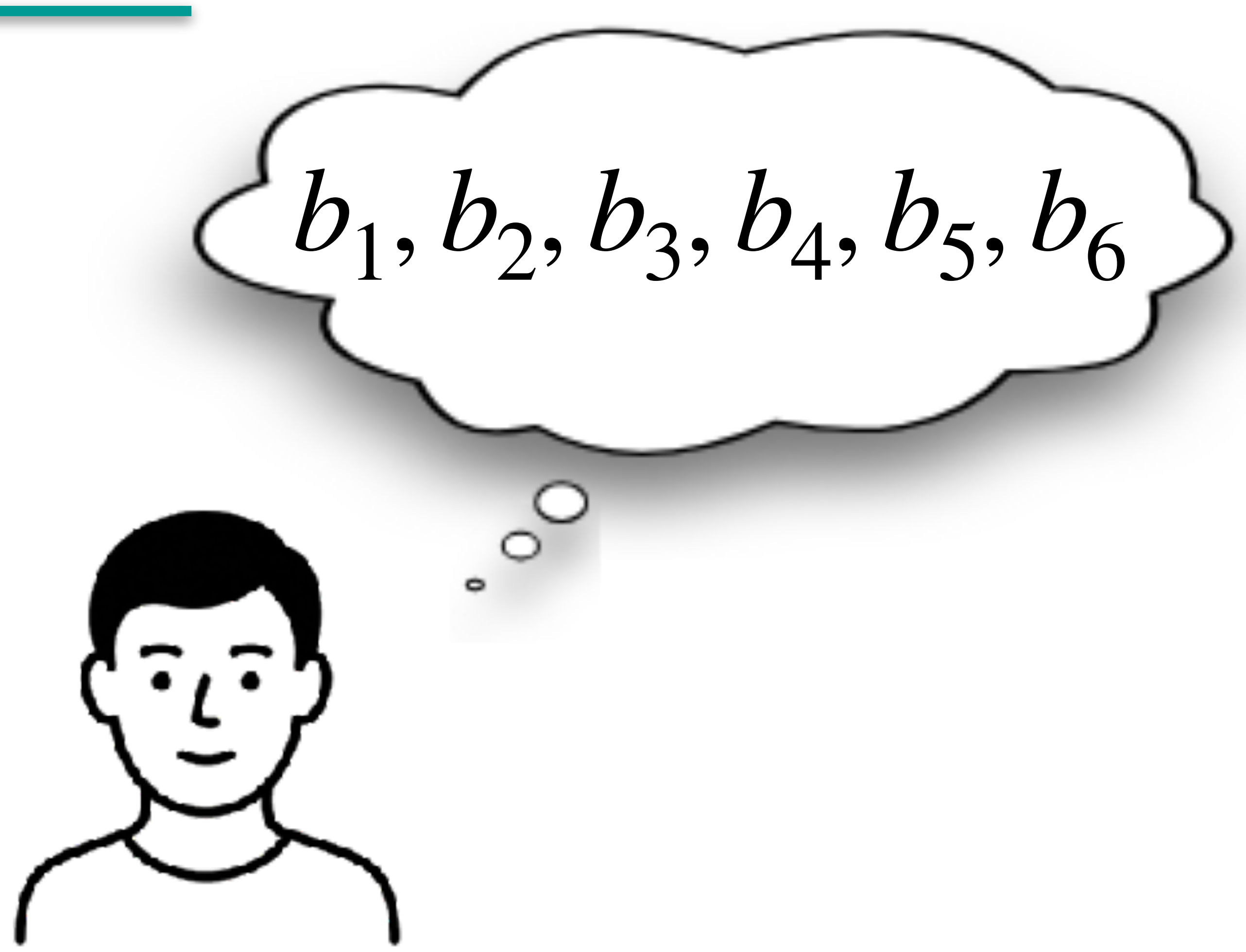
Transferts Inconscients corrélés



u_1	$u_1 + \delta_1$
u_2	$u_2 + \delta_2$
u_3	$u_3 + \delta_3$
u_4	$u_4 + \delta_4$
u_5	$u_5 + \delta_5$
u_6	$u_6 + \delta_6$

$$\begin{array}{l} u_1 + b_1 \cdot \delta_1 \\ u_2 + b_2 \cdot \delta_2 \\ u_3 + b_3 \cdot \delta_3 \\ u_4 + b_4 \cdot \delta_4 \\ u_5 + b_5 \cdot \delta_5 \\ u_6 + b_6 \cdot \delta_6 \end{array}$$

Transferts Inconscients corrélés

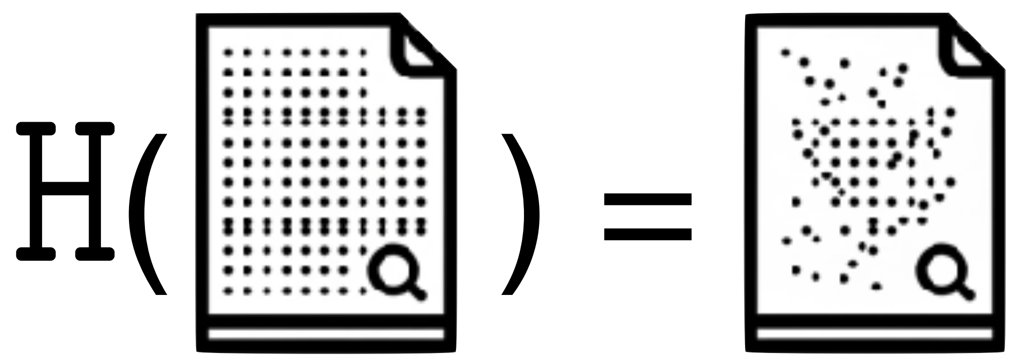


u_1	$u_1 + \delta$
u_2	$u_2 + \delta$
u_3	$u_3 + \delta$
u_4	$u_4 + \delta$
u_5	$u_5 + \delta$
u_6	$u_6 + \delta$

$$u_1 + b_1 \cdot \delta$$
$$u_2 + b_2 \cdot \delta$$
$$u_3 + b_3 \cdot \delta$$
$$u_4 + b_4 \cdot \delta$$
$$u_5 + b_5 \cdot \delta$$
$$u_6 + b_6 \cdot \delta$$

Interlude II : fonctions de hachage

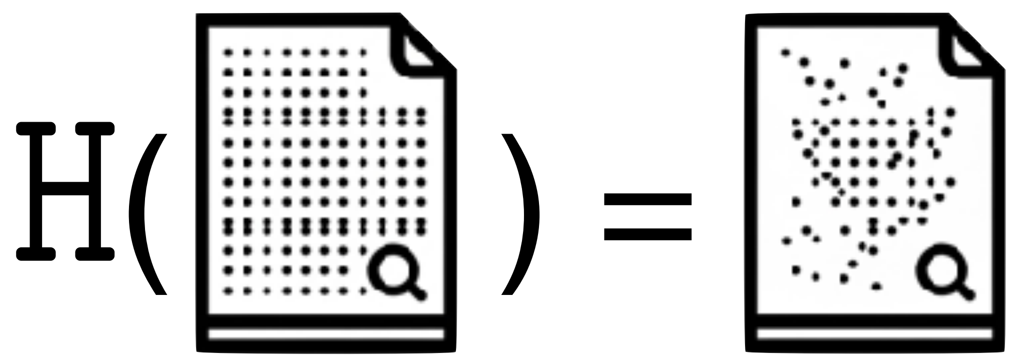
Une fonction de hachage $\mathtt{H}$ prend en entrée un document x de taille arbitraire et renvoie une chaîne y de taille fixée.



Dans une « bonne » fonction de hachage $\mathtt{H}$, quelle que soit l'entrée, la sortie doit avoir l'air « aléatoire ».

Interlude II : fonctions de hachage

Une fonction de hachage $\mathtt{H}$ prend en entrée un document x de taille arbitraire et renvoie une chaîne y de taille fixée.

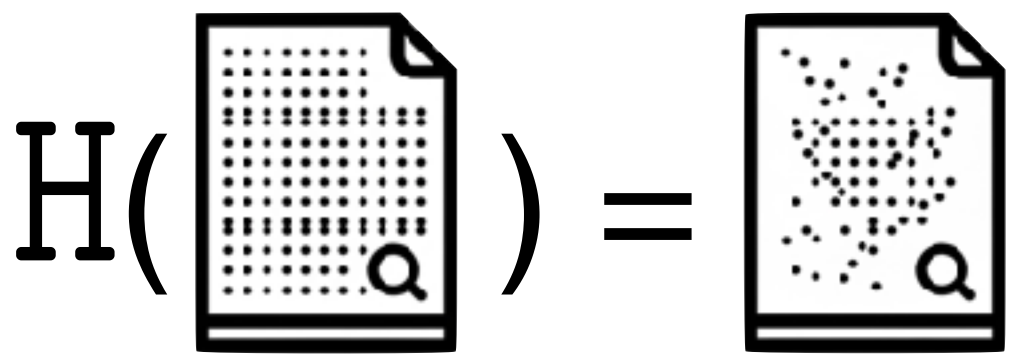


Dans une « bonne » fonction de hachage $\mathtt{H}$, quelle que soit l'entrée, la sortie doit avoir l'air « aléatoire ».

$\mathtt{H}$ est **robuste aux corrélations** si :

Interlude II : fonctions de hachage

Une fonction de hachage $\mathtt{H}$ prend en entrée un document x de taille arbitraire et renvoie une chaîne y de taille fixée.



Dans une « bonne » fonction de hachage $\mathtt{H}$, quelle que soit l'entrée, la sortie doit avoir l'air « aléatoire ».

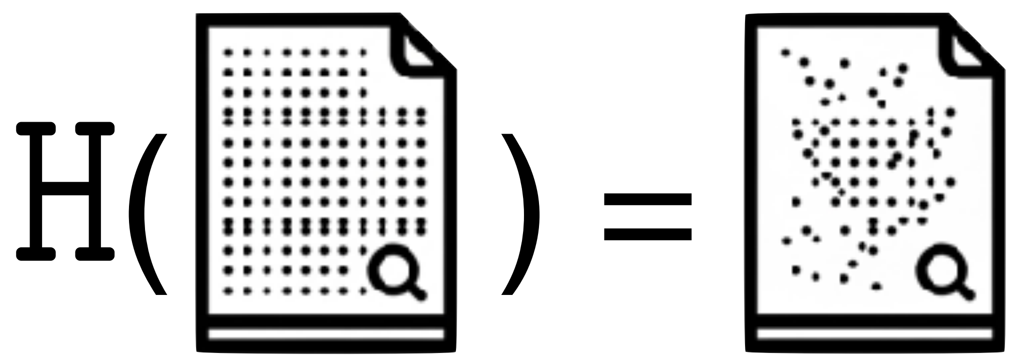
$\mathtt{H}$ est **robuste aux corrélations** si :

$u_0 + \delta$ $\quad$ $u_1 + \delta$ $\quad$ $u_2 + \delta$

u_0 $\quad$ u_1 $\quad$ u_2

Interlude II : fonctions de hachage

Une fonction de hachage $\mathtt{H}$ prend en entrée un document x de taille arbitraire et renvoie une chaîne y de taille fixée.



Dans une « bonne » fonction de hachage $\mathtt{H}$, quelle que soit l'entrée, la sortie doit avoir l'air « aléatoire ».

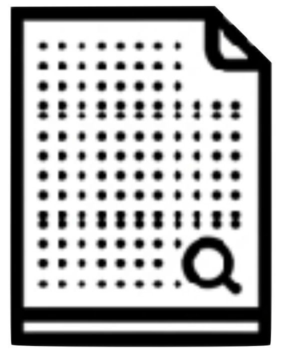
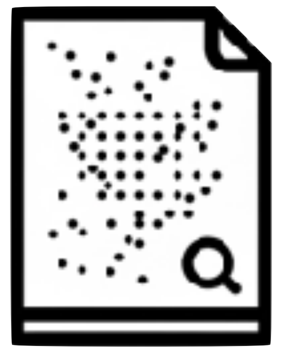
$\mathtt{H}$ est **robuste aux corrélations** si :

$$\mathtt{H}(u_0 + \delta) \qquad \mathtt{H}(u_1 + \delta) \qquad \mathtt{H}(u_2 + \delta)$$

$$u_0 \qquad u_1 \qquad u_2$$

Interlude II : fonctions de hachage

Une fonction de hachage $\mathtt{H}$ prend en entrée un document x de taille arbitraire et renvoie une chaîne y de taille fixée.

$\mathtt{H}($  $) =$ 

Dans une « bonne » fonction de hachage $\mathtt{H}$, quelle que soit l'entrée, la sortie doit avoir l'air « aléatoire ».

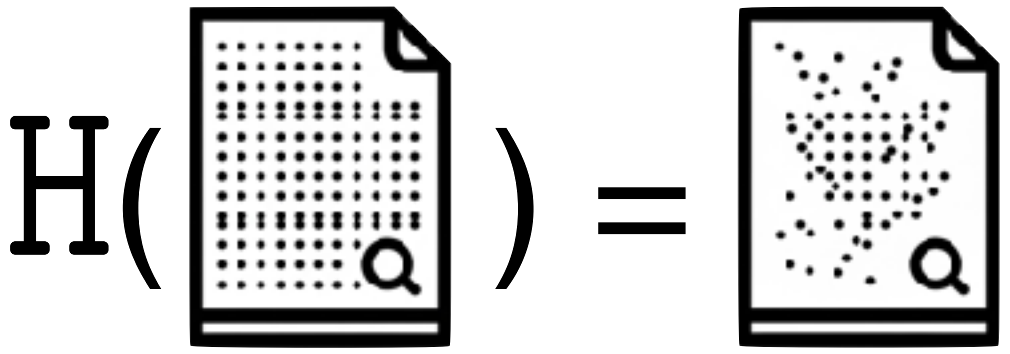
$\mathtt{H}$ est **robuste aux corrélations** si :

$$\mathtt{H}(u_0 + \delta) \quad \mathtt{H}(u_1 + \delta) \quad \mathtt{H}(u_2 + \delta) \approx \text{aléa}$$

$u_0 \qquad u_1 \qquad u_2$

Interlude II : fonctions de hachage

Une fonction de hachage $\mathtt{H}$ prend en entrée un document x de taille arbitraire et renvoie une chaîne y de taille fixée.



Dans une « bonne » fonction de hachage $\mathtt{H}$, quelle que soit l'entrée, la sortie doit avoir l'air « aléatoire ».

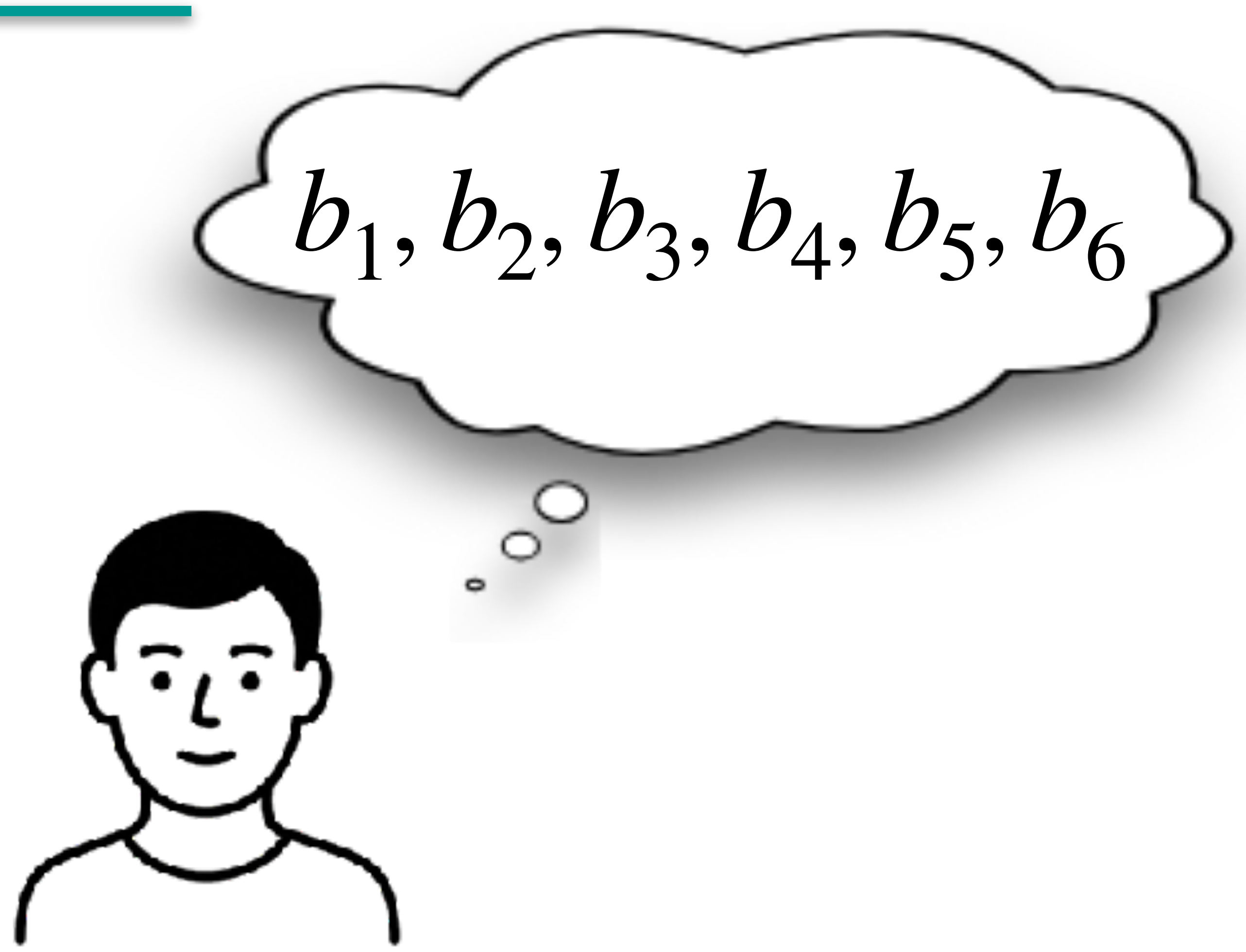
$\mathtt{H}$ est **robuste aux corrélations** si :

$$\mathtt{H}(u_0+\delta) \quad \mathtt{H}(u_1+\delta) \quad \mathtt{H}(u_2+\delta) \quad \approx \quad \text{aléa}$$

$$u_0 \qquad u_1 \qquad u_2$$

Fonctionne seulement si δ a une entropie suffisante (par exemple, 128 bits)

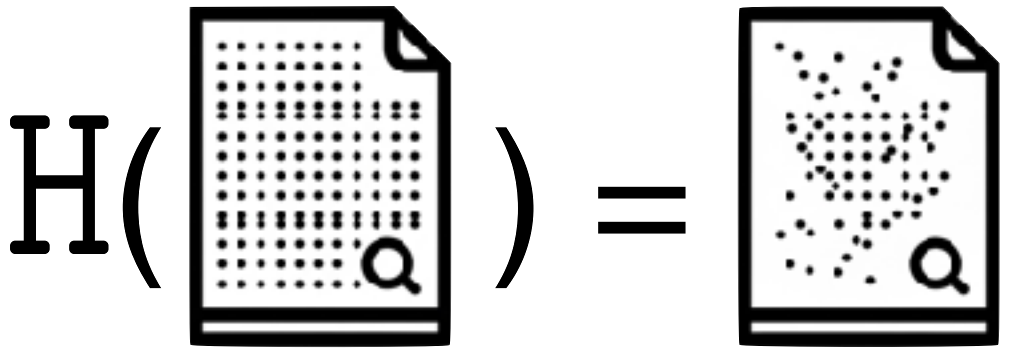
Transferts Inconscients corrélés



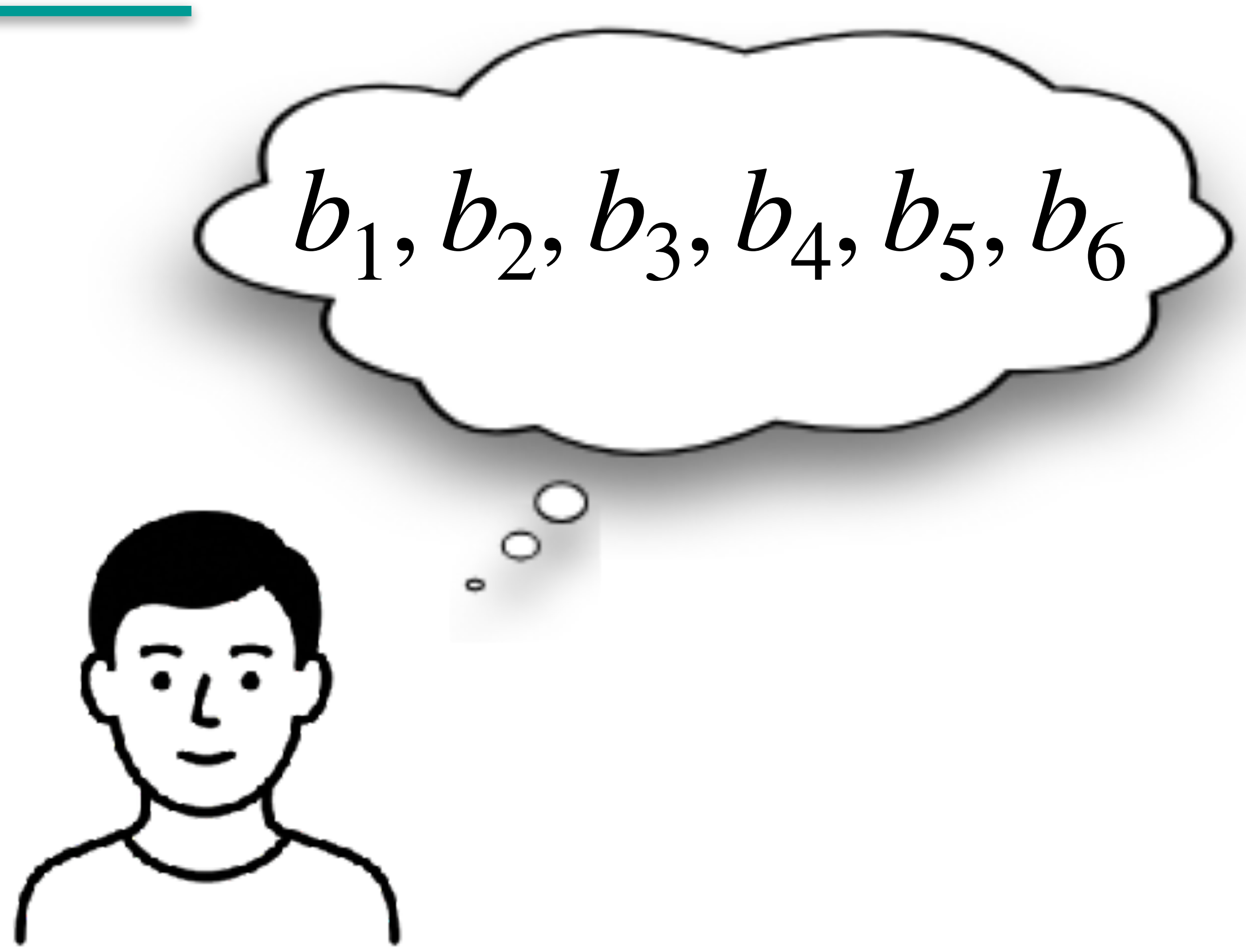
u_1	$u_1+\delta$
u_2	$u_2+\delta$
u_3	$u_3+\delta$
u_4	$u_4+\delta$
u_5	$u_5+\delta$
u_6	$u_6+\delta$

$u_1 + b_1 \cdot \delta$
$u_2 + b_2 \cdot \delta$
$u_3 + b_3 \cdot \delta$
$u_4 + b_4 \cdot \delta$
$u_5 + b_5 \cdot \delta$
$u_6 + b_6 \cdot \delta$

Transferts Inconscients corrélés



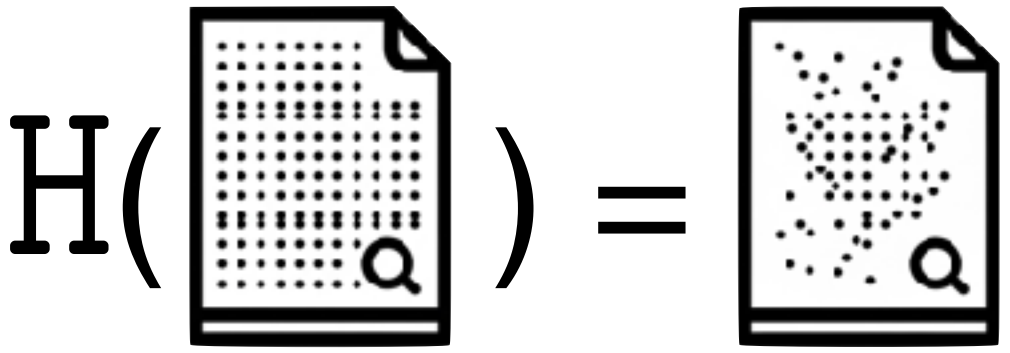
est **robuste aux corrélations**



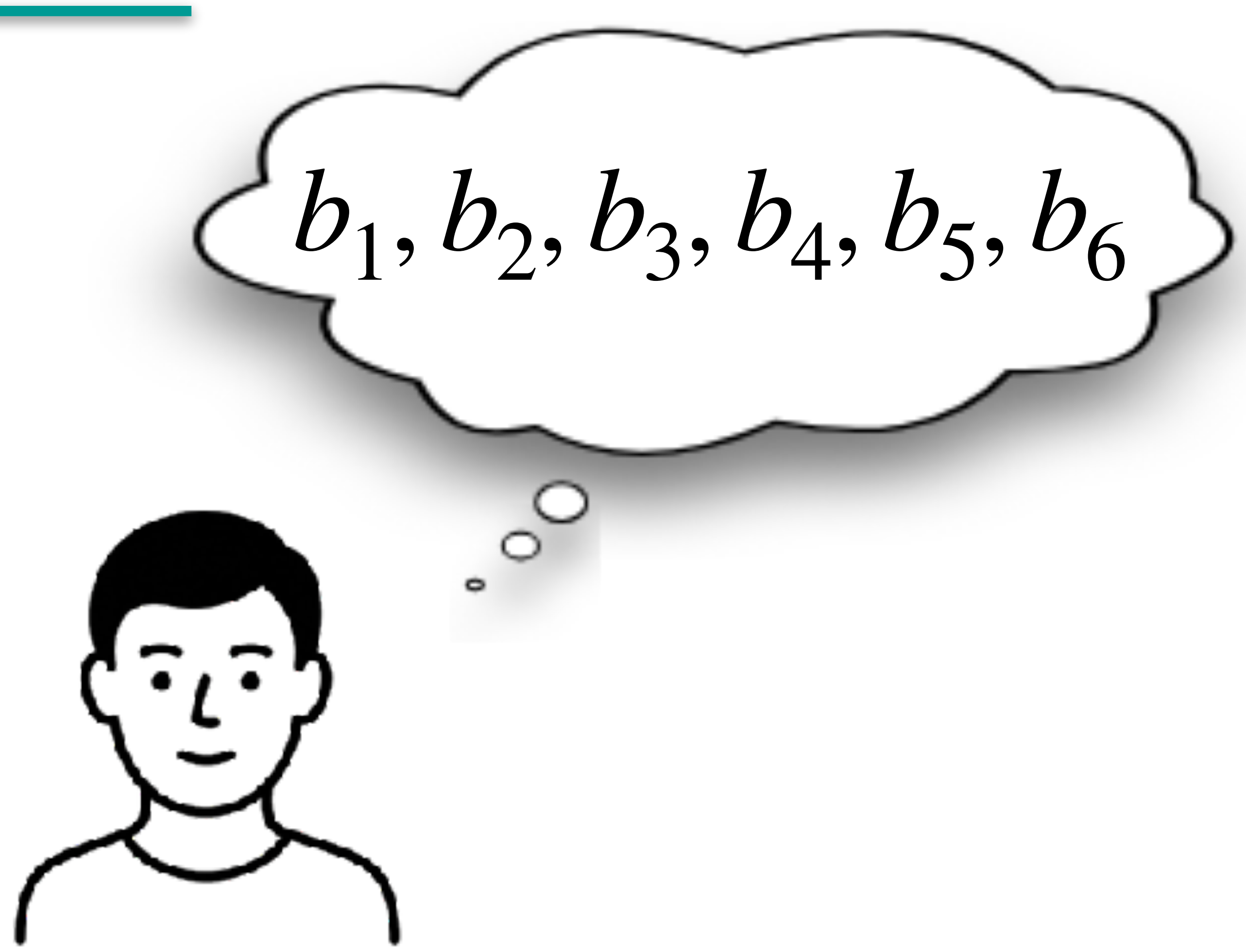
u_1	$u_1+\delta$
u_2	$u_2+\delta$
u_3	$u_3+\delta$
u_4	$u_4+\delta$
u_5	$u_5+\delta$
u_6	$u_6+\delta$

$u_1 + b_1 \cdot \delta$
$u_2 + b_2 \cdot \delta$
$u_3 + b_3 \cdot \delta$
$u_4 + b_4 \cdot \delta$
$u_5 + b_5 \cdot \delta$
$u_6 + b_6 \cdot \delta$

Transferts Inconscients corrélés



est **robuste aux corrélations**

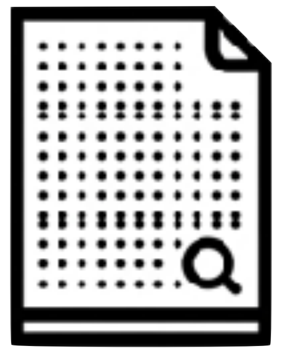
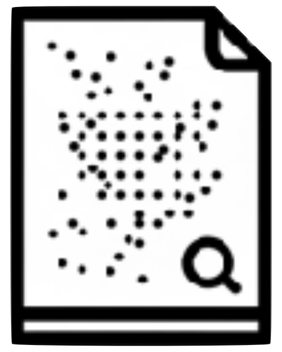


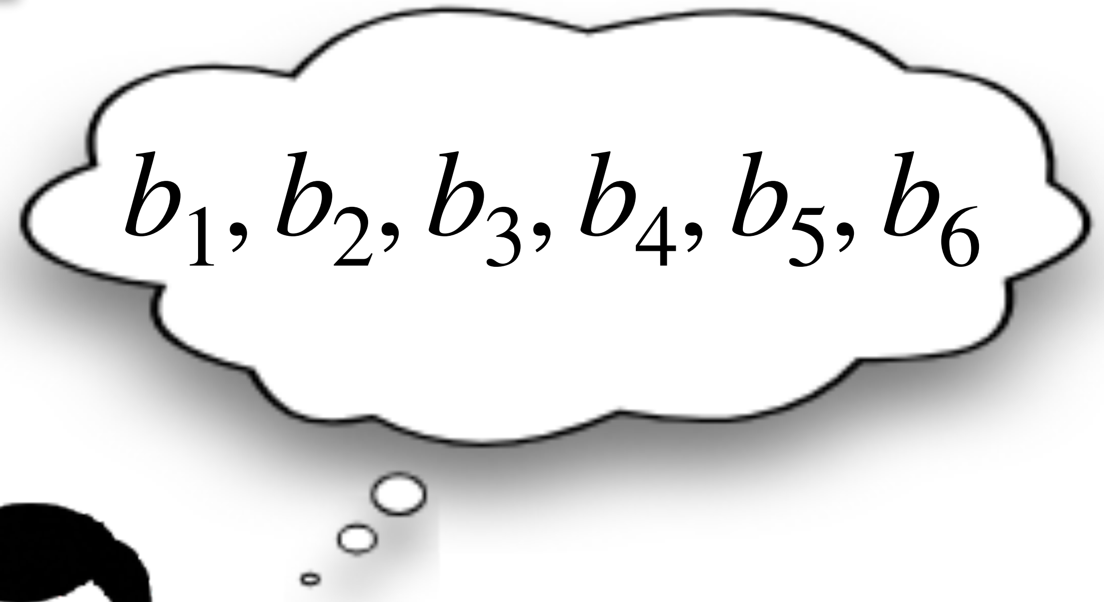
En hachant la sortie, Alice et Bob « décorrèlent » les transferts inconscients corrélés et obtiennent des transferts inconscients classiques sur des données « aléatoires »

$\mathrm{H}(u_1)$	$\mathrm{H}(u_1+\delta)$
$\mathrm{H}(u_2)$	$\mathrm{H}(u_2+\delta)$
$\mathrm{H}(u_3)$	$\mathrm{H}(u_3+\delta)$
$\mathrm{H}(u_4)$	$\mathrm{H}(u_4+\delta)$
$\mathrm{H}(u_5)$	$\mathrm{H}(u_5+\delta)$
$\mathrm{H}(u_6)$	$\mathrm{H}(u_6+\delta)$

$\mathrm{H}(u_1 + b_1 \cdot \delta)$	$= \mathrm{H}(u_1) + b_1 \cdot \mathrm{H}(u_1+\delta)$
$\mathrm{H}(u_2 + b_2 \cdot \delta)$	$\vdots$
$\mathrm{H}(u_3 + b_3 \cdot \delta)$	
$\mathrm{H}(u_4 + b_4 \cdot \delta)$	
$\mathrm{H}(u_5 + b_5 \cdot \delta)$	
$\mathrm{H}(u_6 + b_6 \cdot \delta)$	

Transferts Inconscients corrélés

H() =  est **robuste aux corrélations**



En hachant la sortie, Alice et Bob « décorrèlent » les transferts inconscients corrélés et obtiennent des transferts inconscients classiques sur des données « aléatoires »

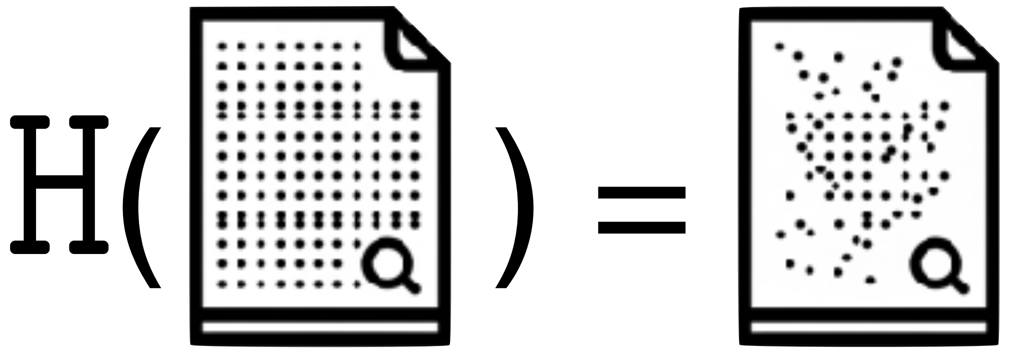
On peut « dérandomiser » ces transferts via le protocole de Beaver

$\mathrm{H}(u_1)$	$\mathrm{H}(u_1+\delta)$
$\mathrm{H}(u_2)$	$\mathrm{H}(u_2+\delta)$
$\mathrm{H}(u_3)$	$\mathrm{H}(u_3+\delta)$
$\mathrm{H}(u_4)$	$\mathrm{H}(u_4+\delta)$
$\mathrm{H}(u_5)$	$\mathrm{H}(u_5+\delta)$
$\mathrm{H}(u_6)$	$\mathrm{H}(u_6+\delta)$

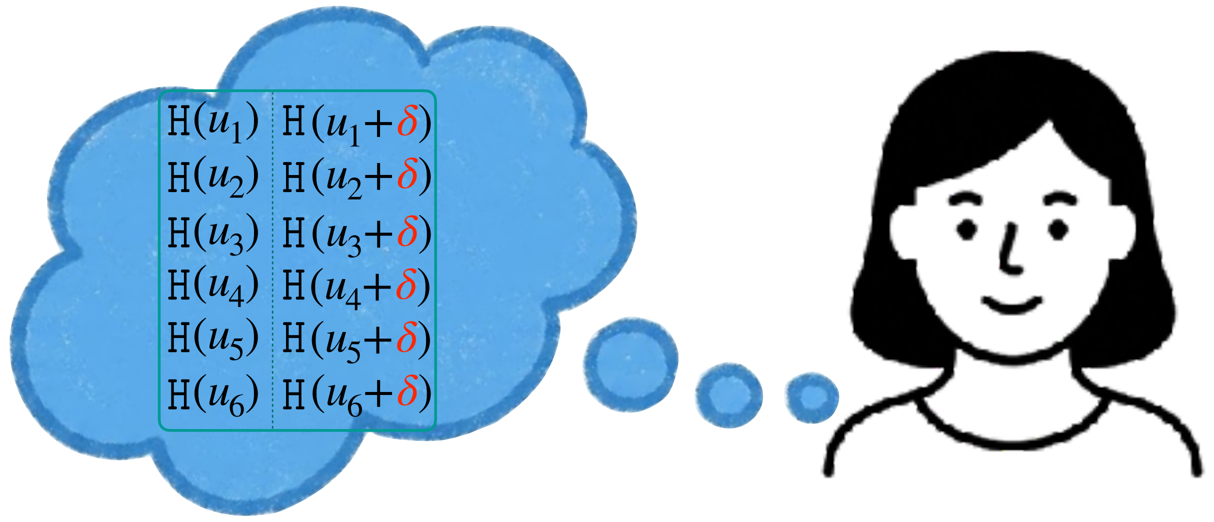
$\mathrm{H}(u_1 + b_1 \cdot \delta)$
$\mathrm{H}(u_2 + b_2 \cdot \delta)$
$\mathrm{H}(u_3 + b_3 \cdot \delta)$
$\mathrm{H}(u_4 + b_4 \cdot \delta)$
$\mathrm{H}(u_5 + b_5 \cdot \delta)$
$\mathrm{H}(u_6 + b_6 \cdot \delta)$

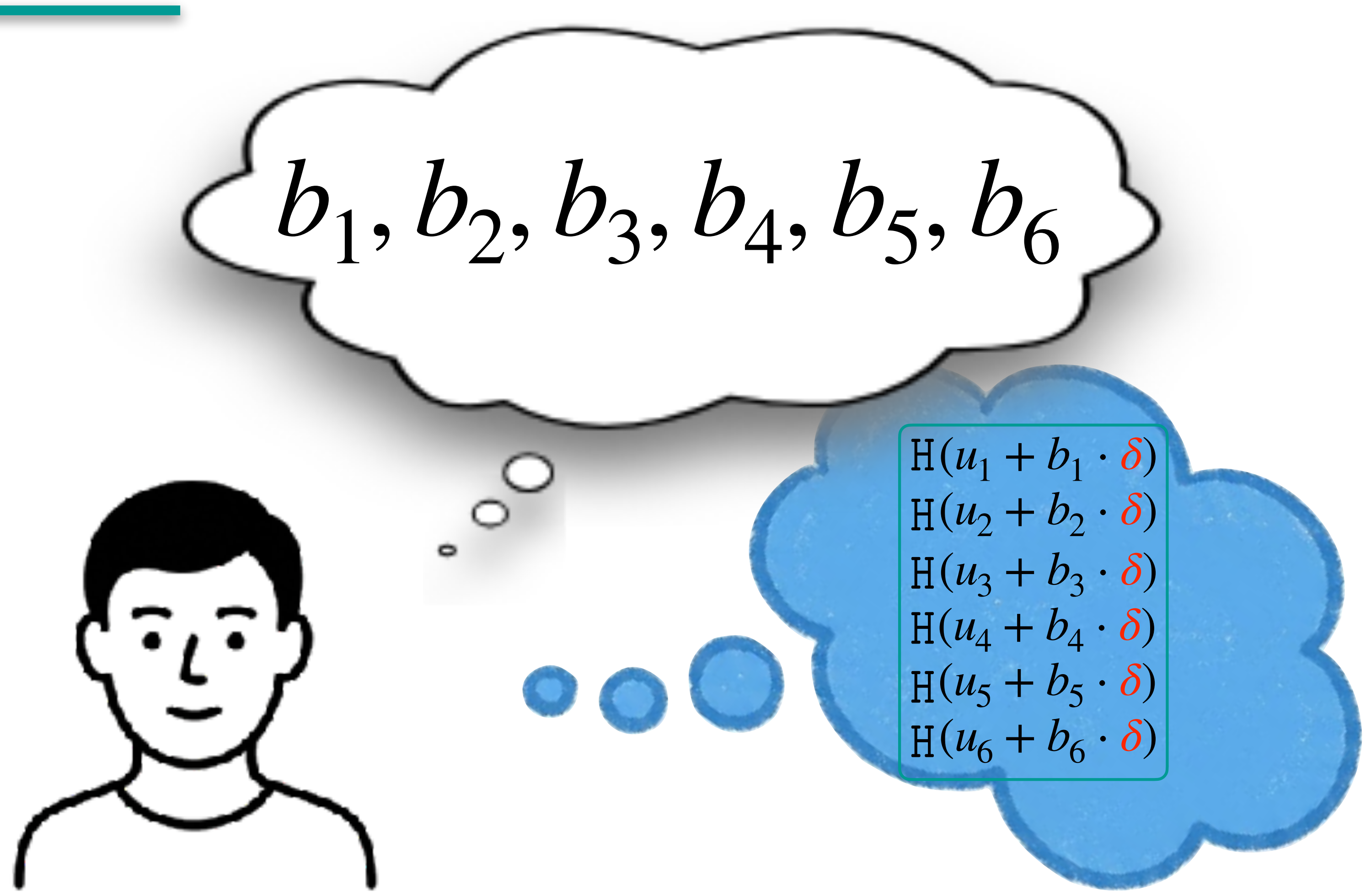
$= \mathrm{H}(u_1) + b_1 \cdot \mathrm{H}(u_1+\delta)$

Transferts Inconscients corrélés



est **robuste aux corrélations**



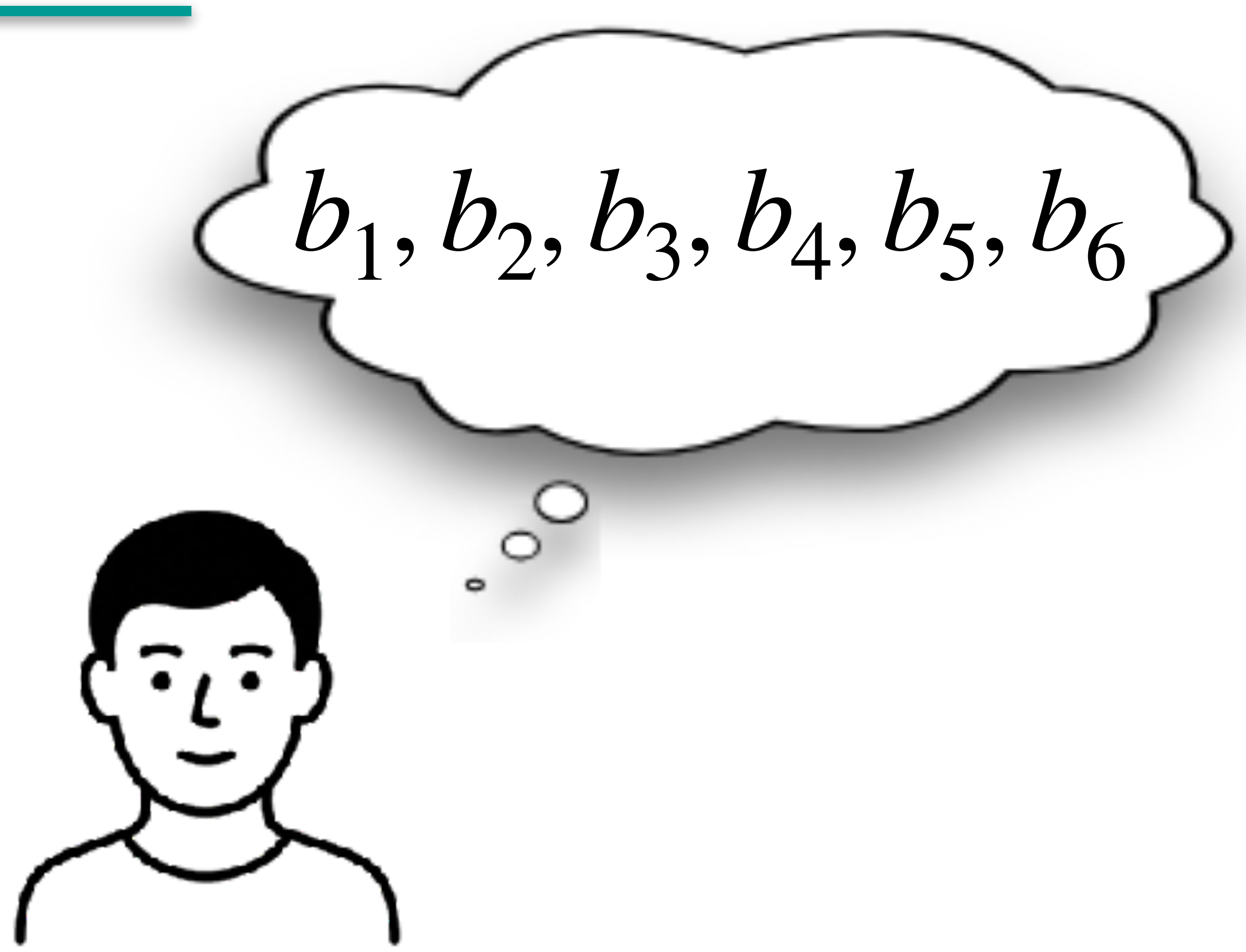


$$= \mathrm{H}(u_1) + b_1 \cdot \mathrm{H}(u_1 + \delta)$$

En hachant la sortie, Alice et Bob « décorrèlent » les transferts inconscients corrélés et obtiennent des transferts inconscients classiques sur des données « aléatoires »

On peut « dérandomiser » ces transferts via le protocole de Beaver

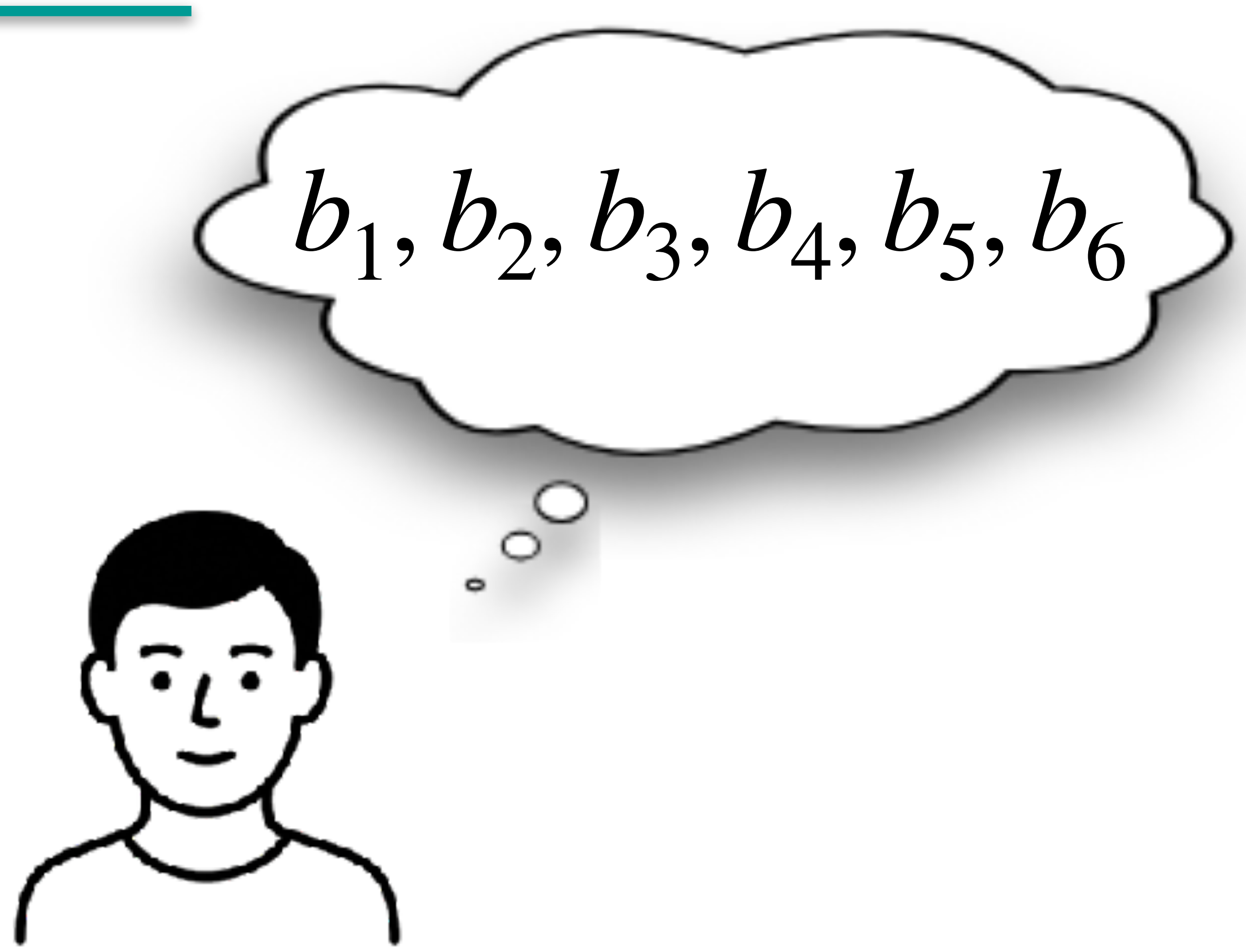
Transferts Inconscients corrélés



u_1	$u_1+\delta$
u_2	$u_2+\delta$
u_3	$u_3+\delta$
u_4	$u_4+\delta$
u_5	$u_5+\delta$
u_6	$u_6+\delta$

$u_1 + b_1 \cdot \delta$
$u_2 + b_2 \cdot \delta$
$u_3 + b_3 \cdot \delta$
$u_4 + b_4 \cdot \delta$
$u_5 + b_5 \cdot \delta$
$u_6 + b_6 \cdot \delta$

Transferts Inconscients corrélés



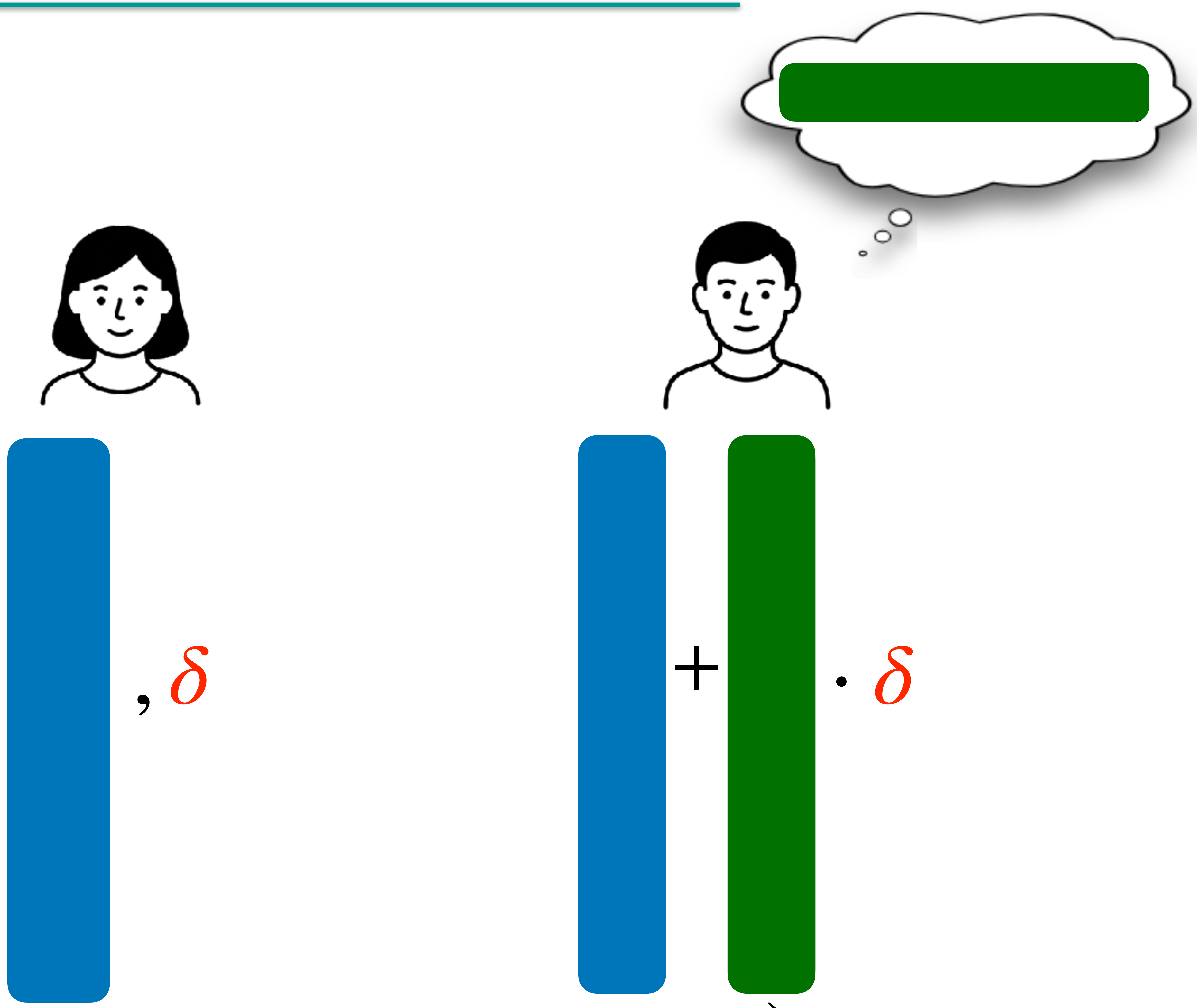
$$\begin{array}{c:c} u_1 & u_1+\delta \\ u_2 & u_2+\delta \\ u_3 & u_3+\delta \\ u_4 & u_4+\delta \\ u_5 & u_5+\delta \\ u_6 & u_6+\delta \end{array}$$

$$\vec{u}$$

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \end{pmatrix} \cdot \delta$$

$$\vec{u} + \vec{b} \cdot \delta$$

Transferts Inconscients corrélés



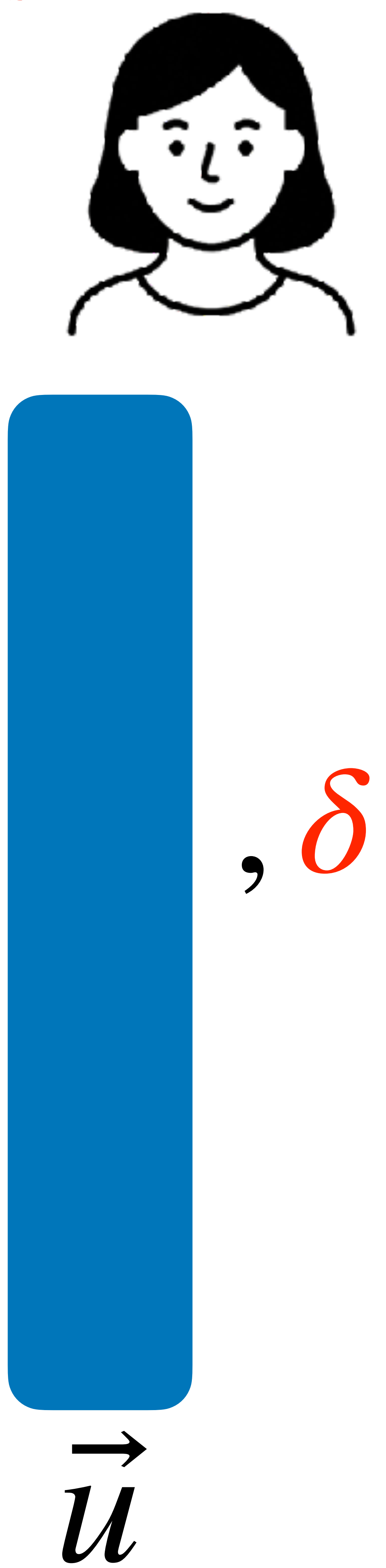
$\vec{u}$

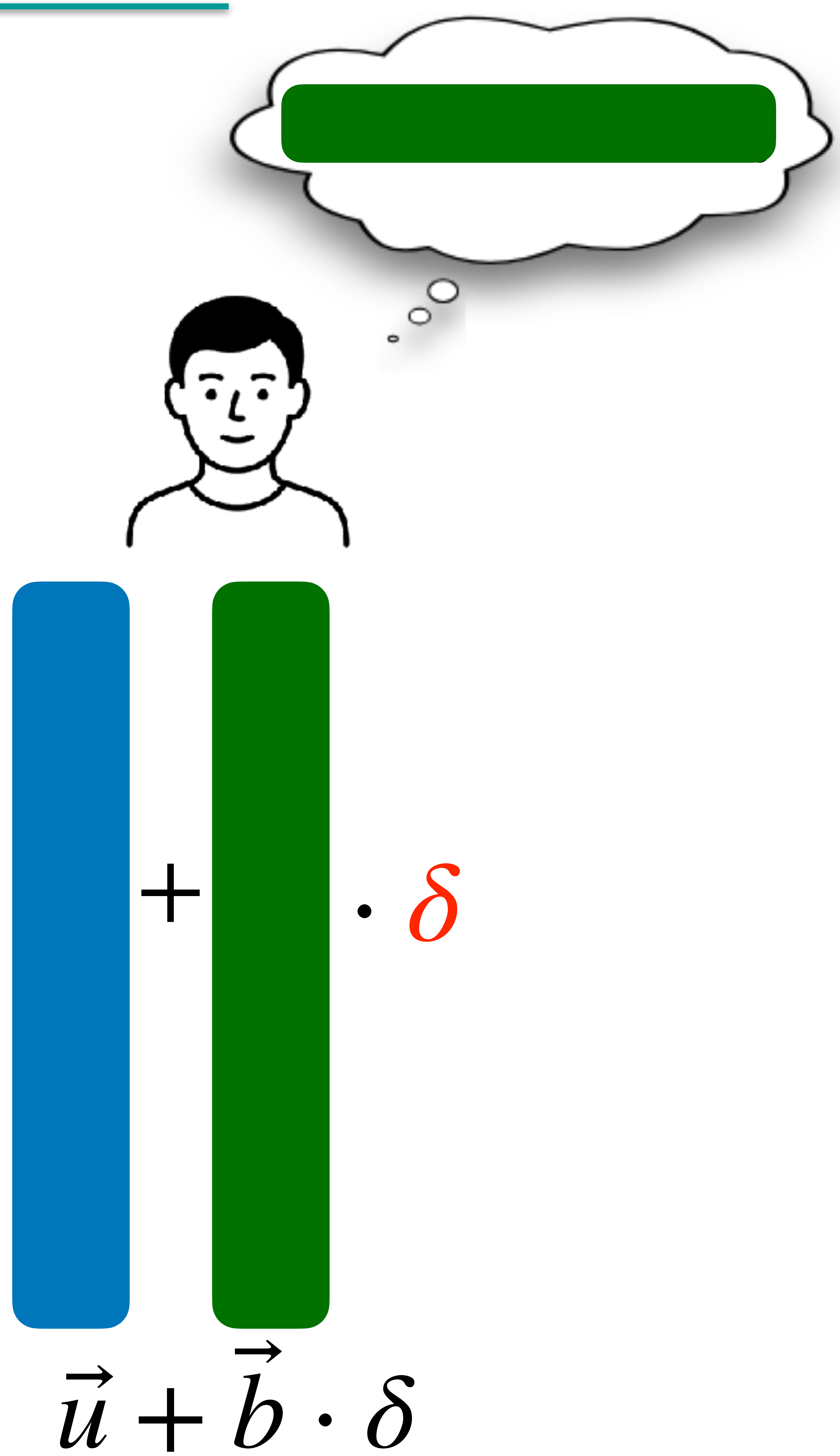
$\vec{u} + \vec{b} \cdot \delta$

Transferts Inconscients corrélés

OBJECTIF 2

Construire des transfers inconscients **corrélés** en grand nombre à partir d'un petit nombre de transfers inconscients



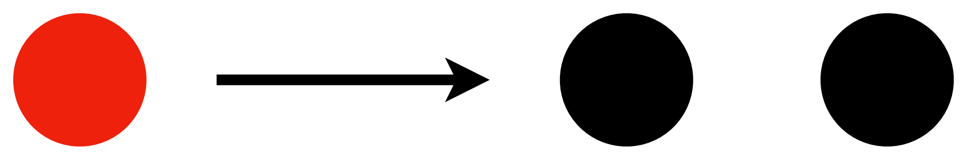


Interlude III : générateur pseudo-aléatoire (PRG)

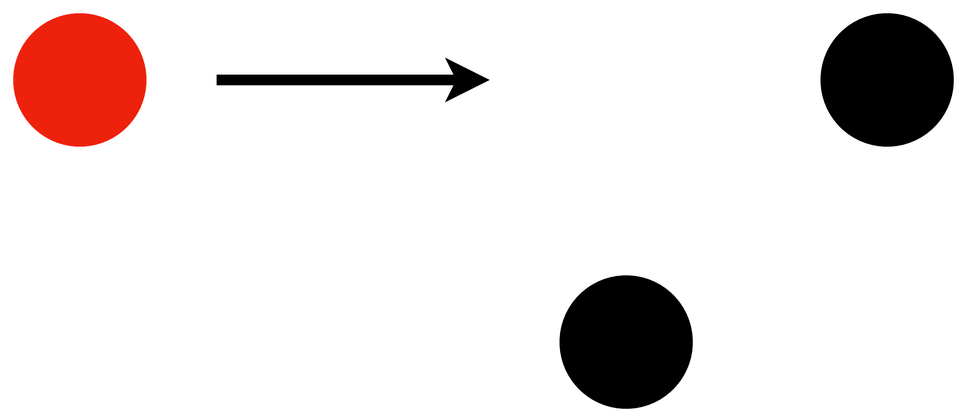
Un générateur $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ prend en entrée une « graine » $x \in \{0,1\}^n$ et produit une sortie $y = G(x)$ plus longue (ici, $|y| = 2n$)

Un générateur $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ est *pseudo-aléatoire* s'il est impossible de distinguer $y = G(x)$ (calculé à partir d'un x aléatoire dans $\{0,1\}^n$) d'une chaîne uniforme y prise dans $\{0,1\}^{2n}$.

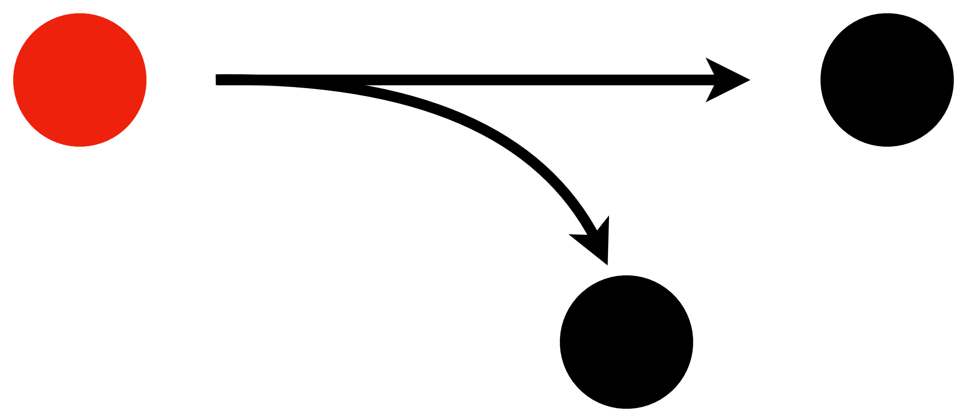
Interlude III : extension d’un PRG « par flot »



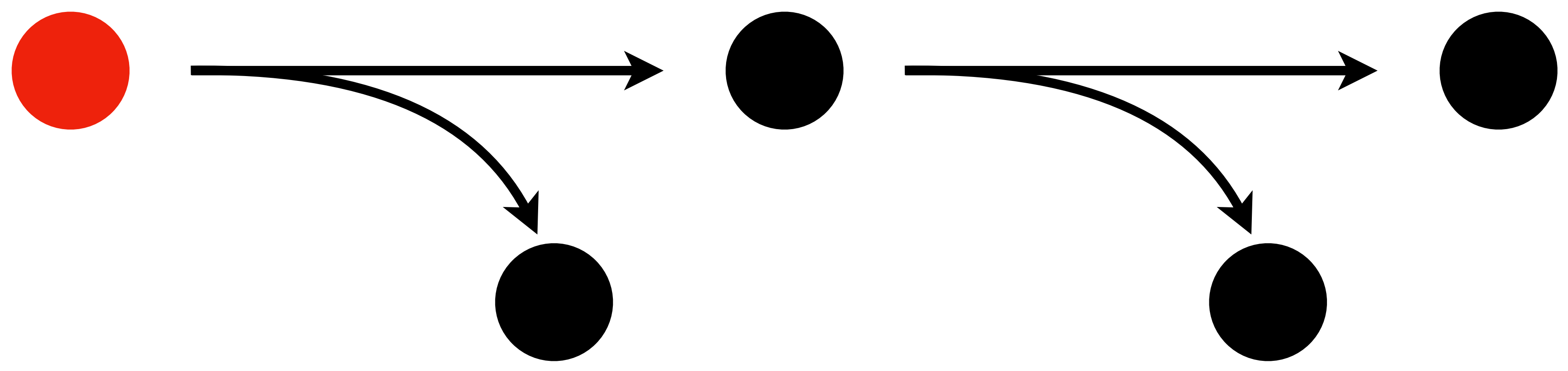
Interlude III : extension d’un PRG « par flot »



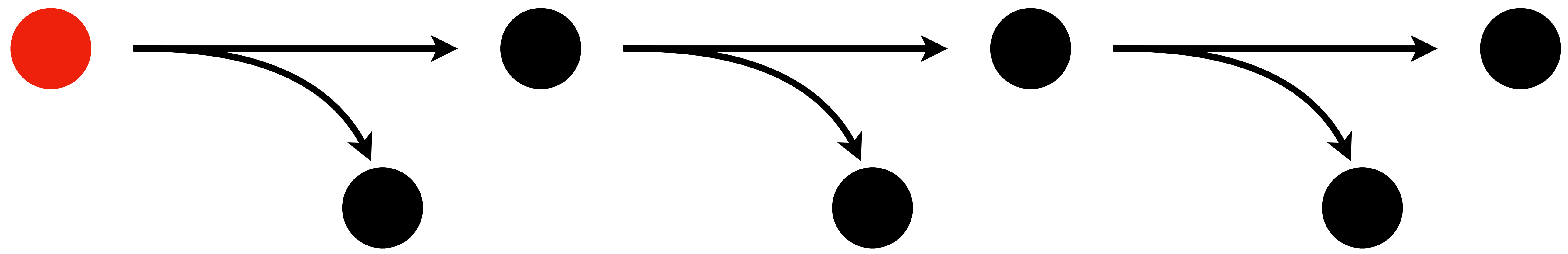
Interlude III : extension d'un PRG « par flot »



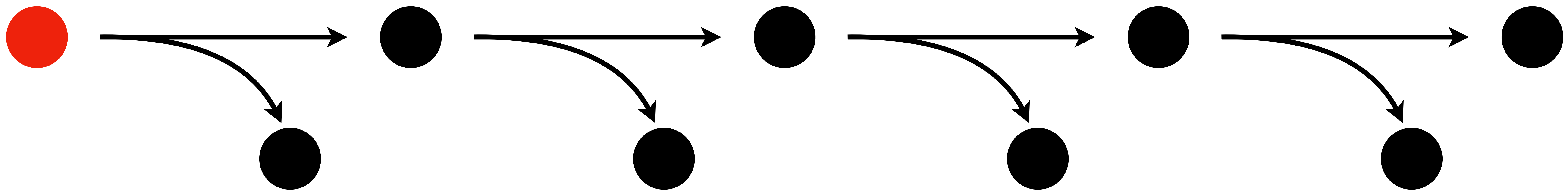
Interlude III : extension d'un PRG « par flot »



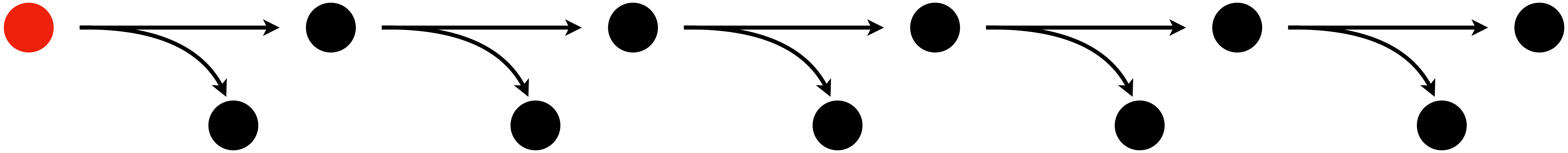
Interlude III : extension d'un PRG « par flot »



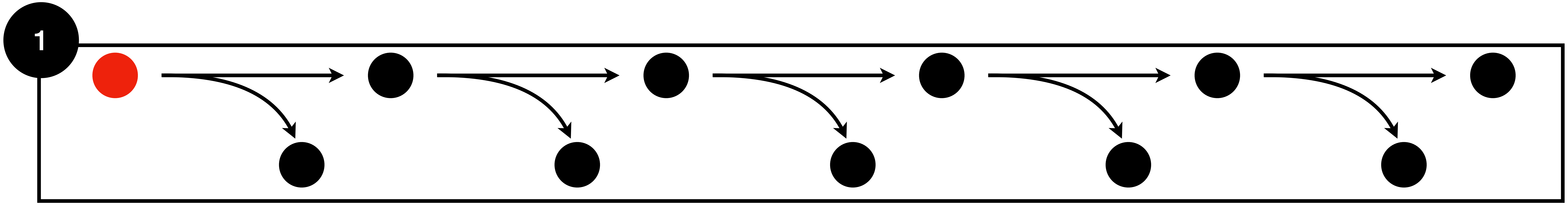
Interlude III : extension d'un PRG « par flot »

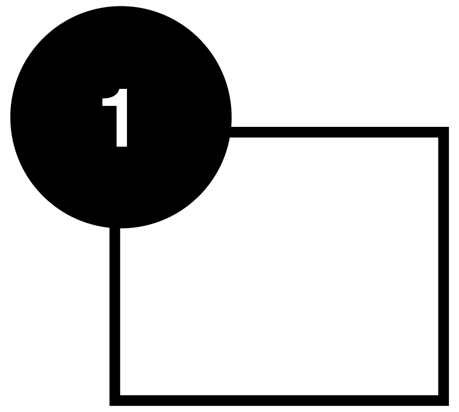


Interlude III : extension d’un PRG « par flot »

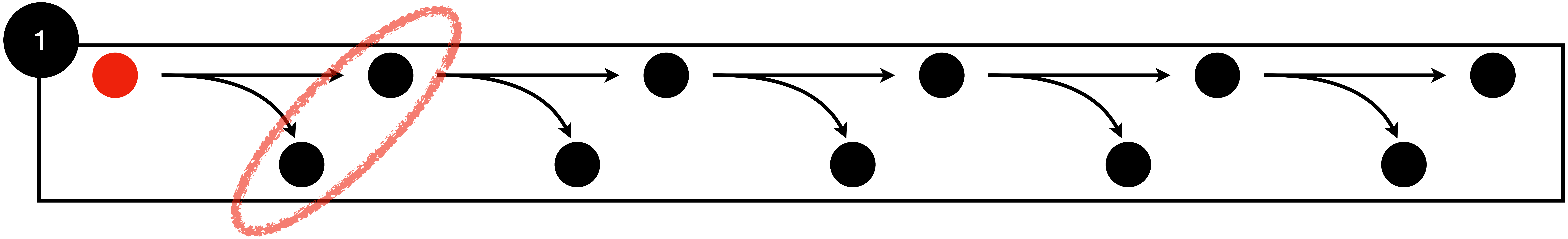


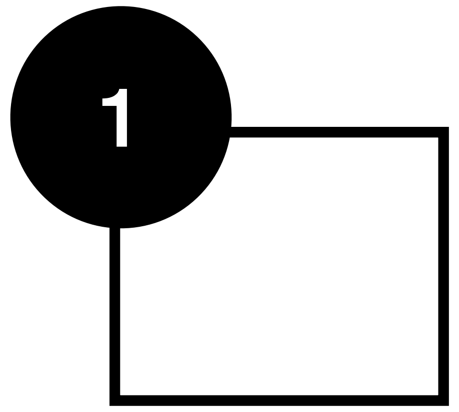
Interlude III : extension d’un PRG « par flot »



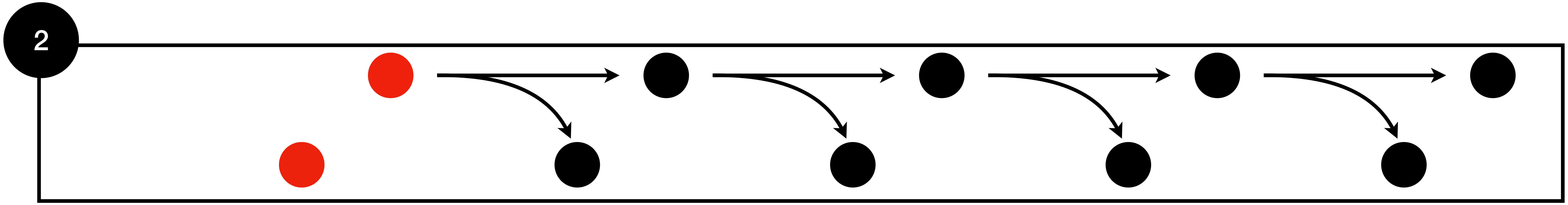


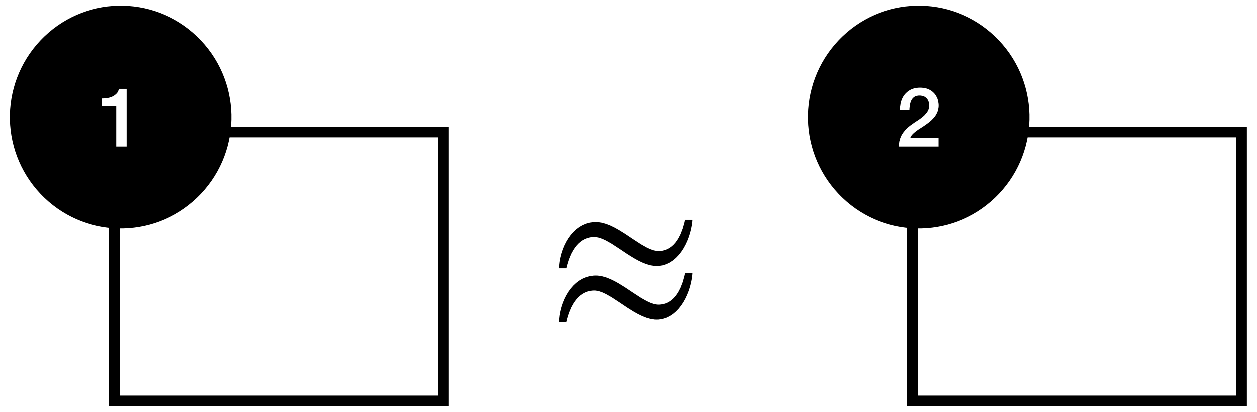
Interlude III : extension d'un PRG « par flot »



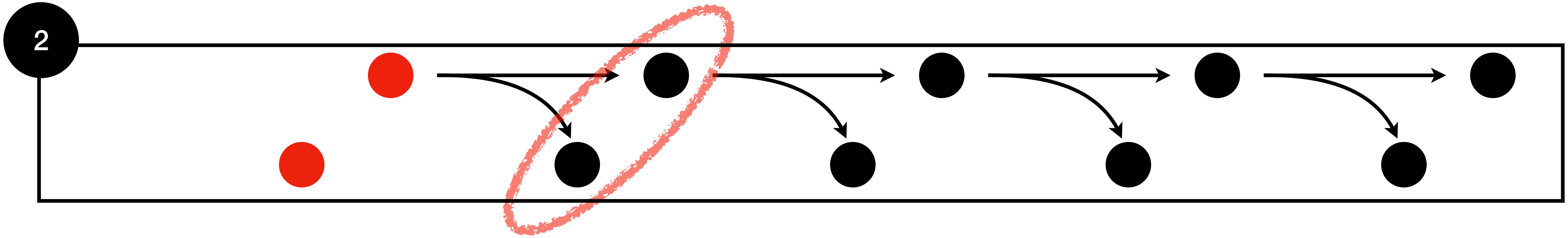


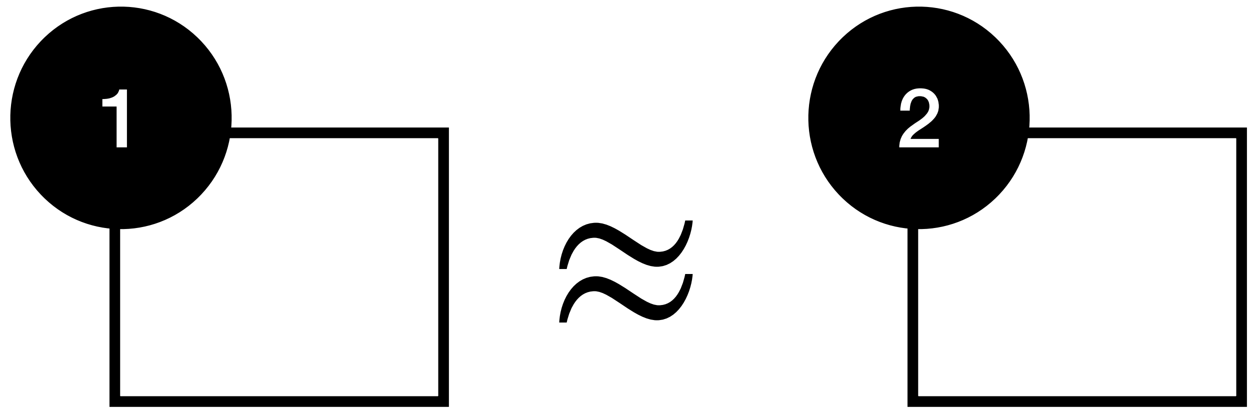
Interlude III : extension d’un PRG « par flot »



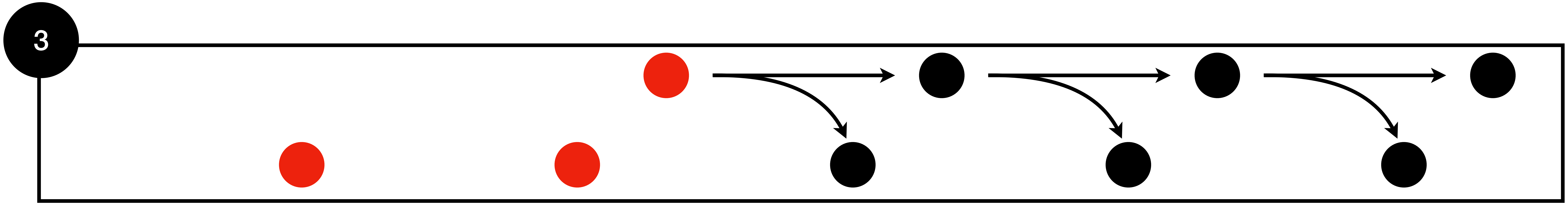


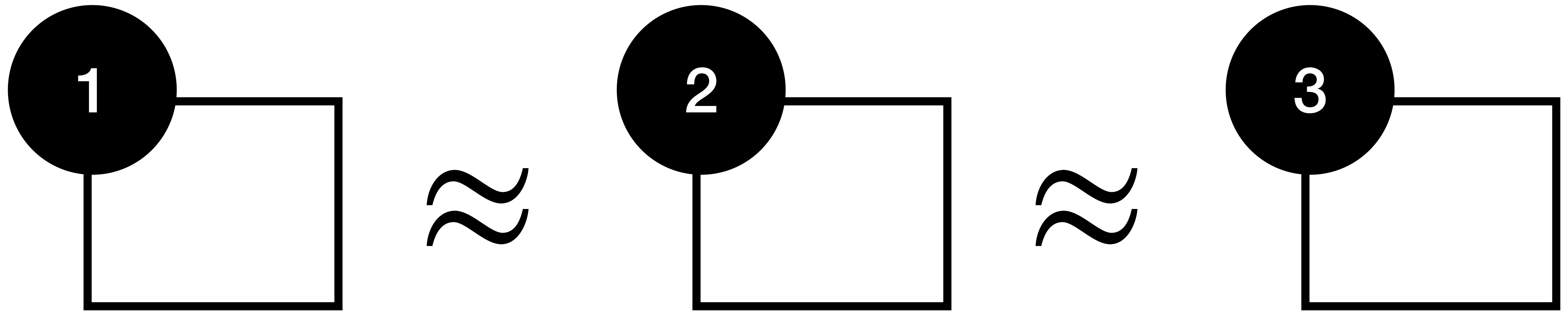
Interlude III : extension d'un PRG « par flot »



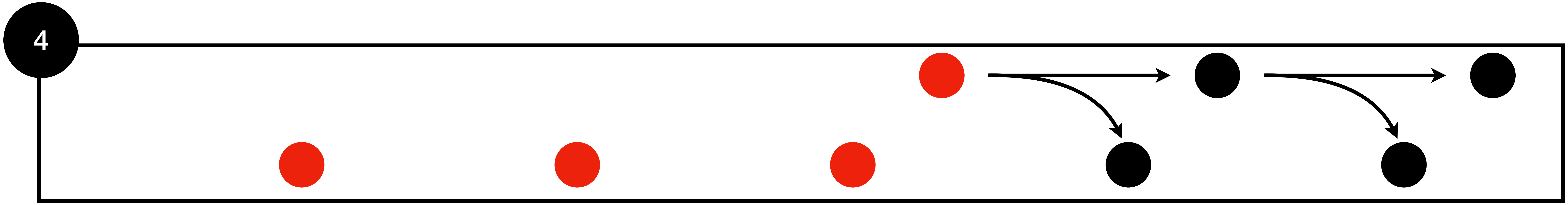


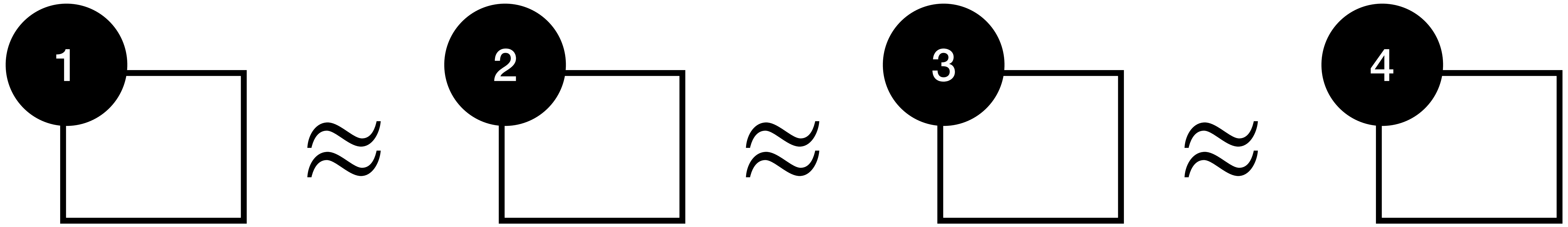
Interlude III : extension d’un PRG « par flot »



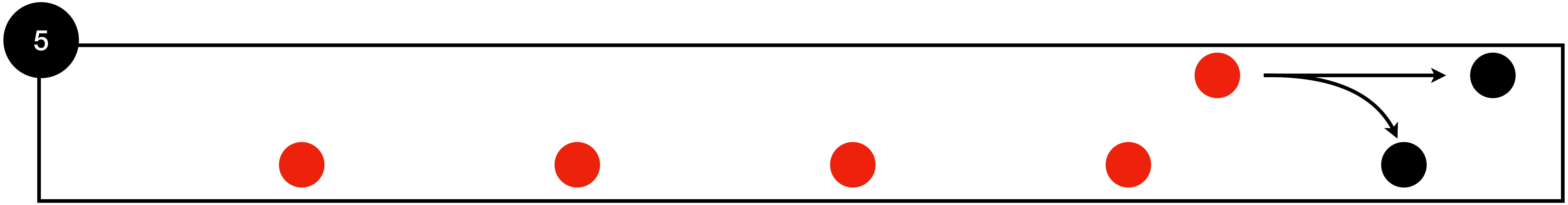


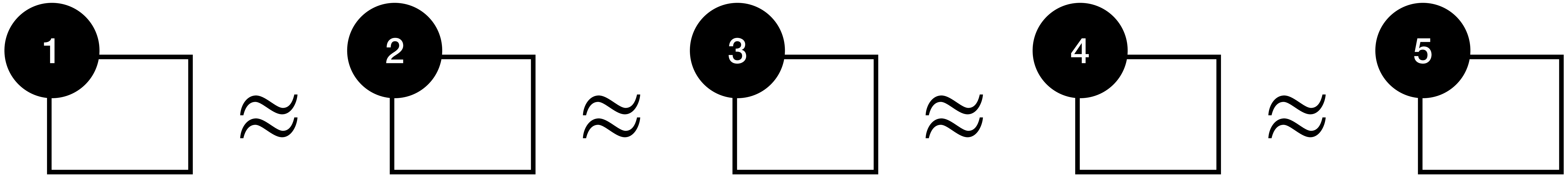
Interlude III : extension d'un PRG « par flot »



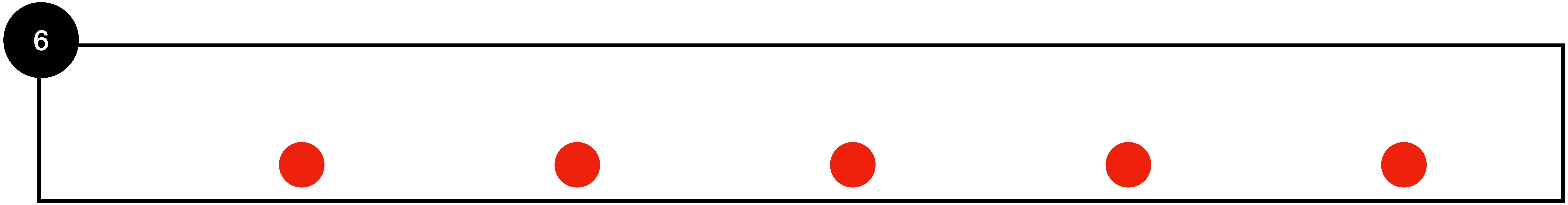


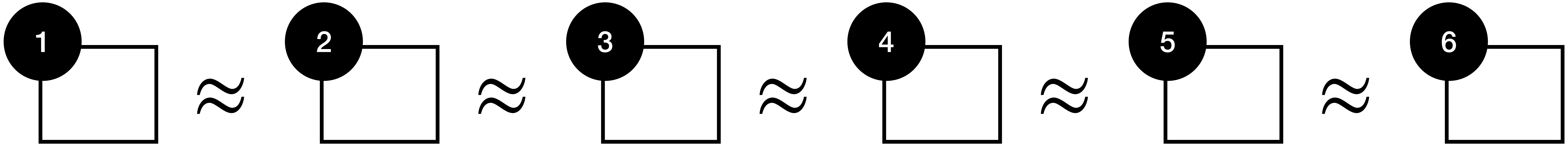
Interlude III : extension d'un PRG « par flot »



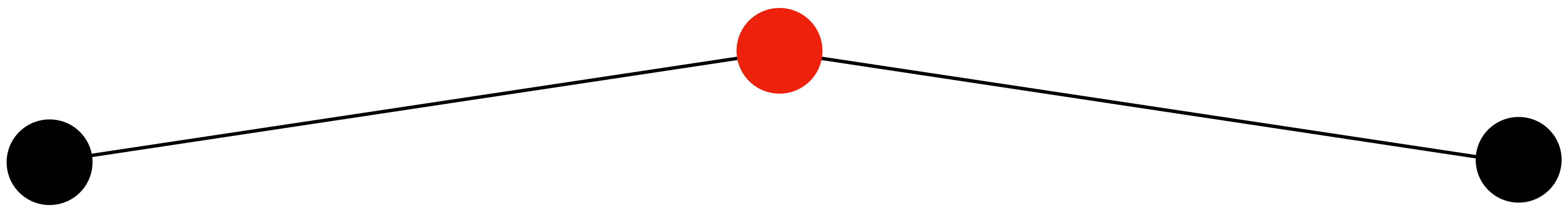


Interlude III : extension d'un PRG « par flot »

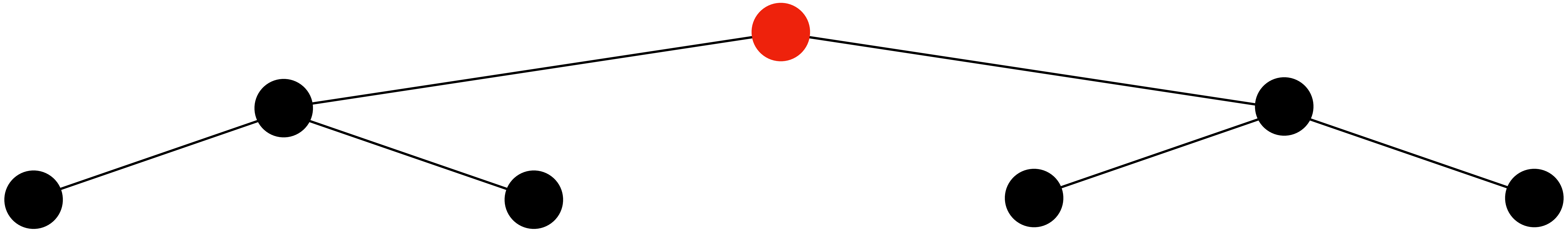




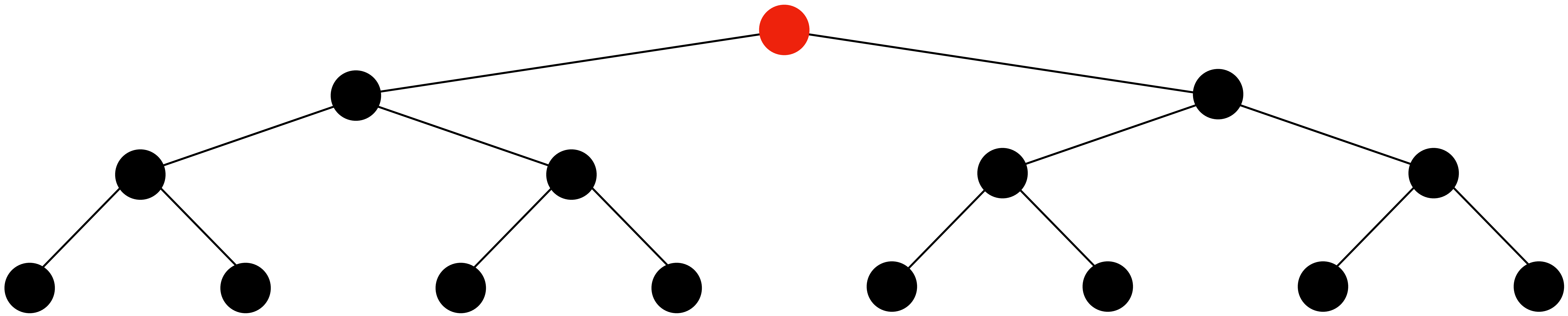
Arbre GGM (Goldreich, Goldwasser, Micali)



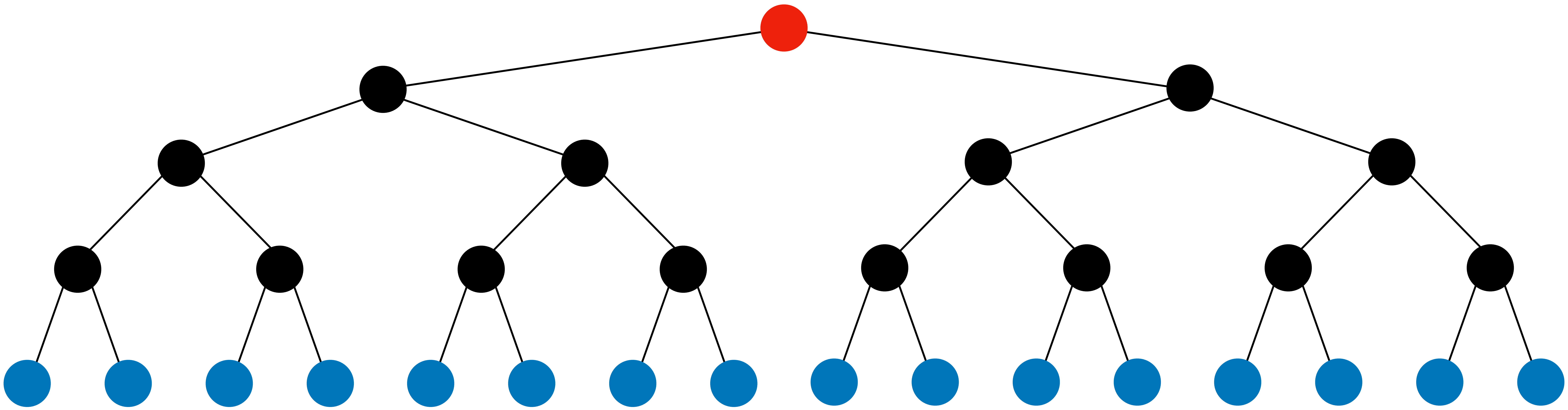
Arbre GGM (Goldreich, Goldwasser, Micali)



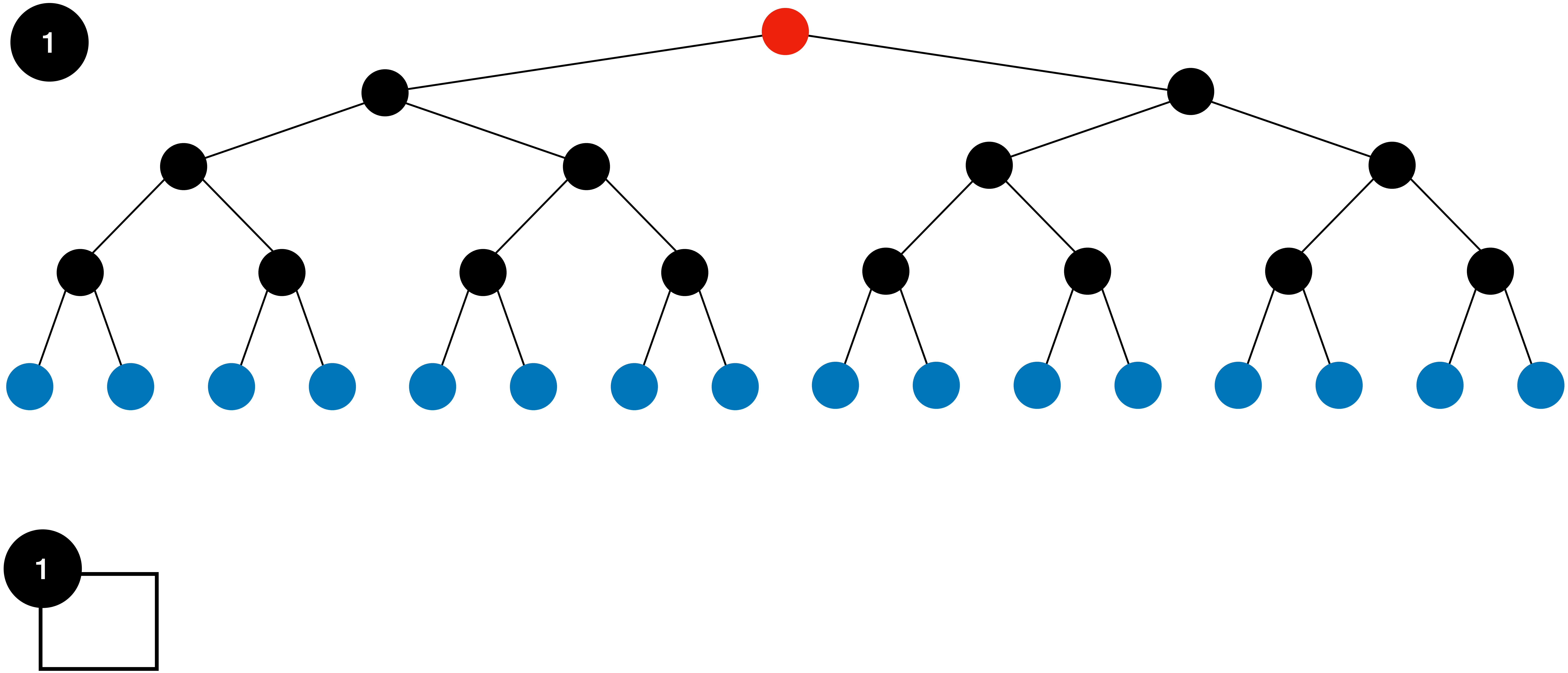
Arbre GGM (Goldreich, Goldwasser, Micali)



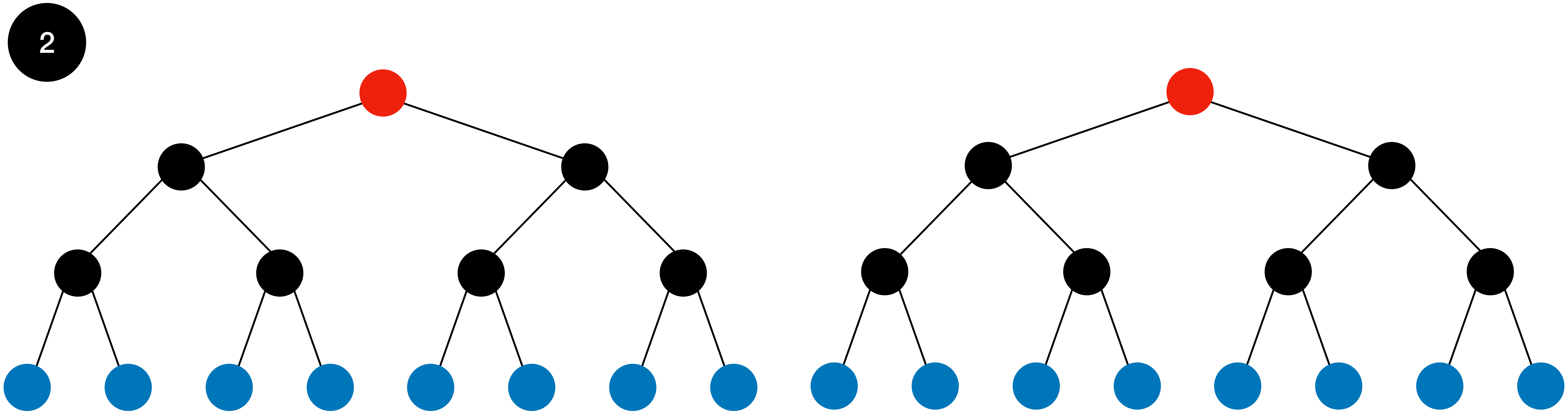
Arbre GGM (Goldreich, Goldwasser, Micali)

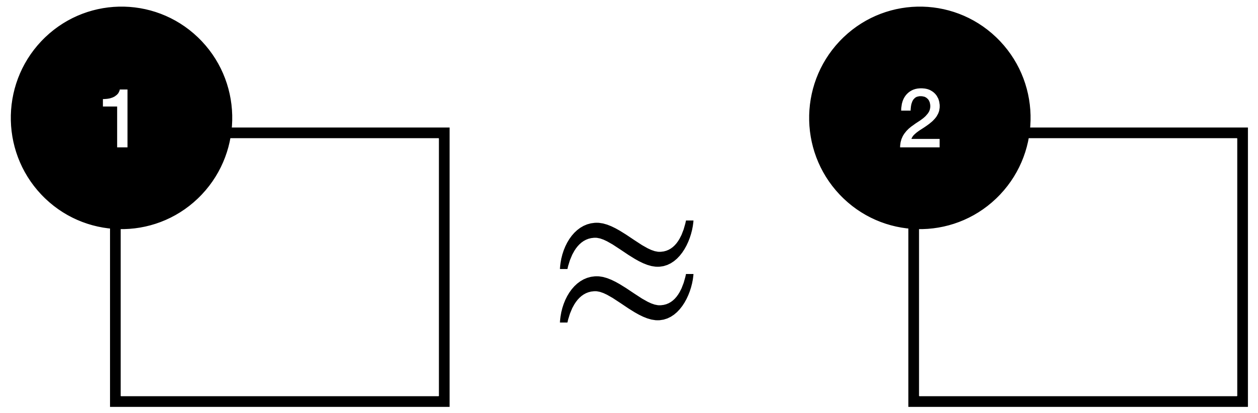


Arbre GGM (Goldreich, Goldwasser, Micali)



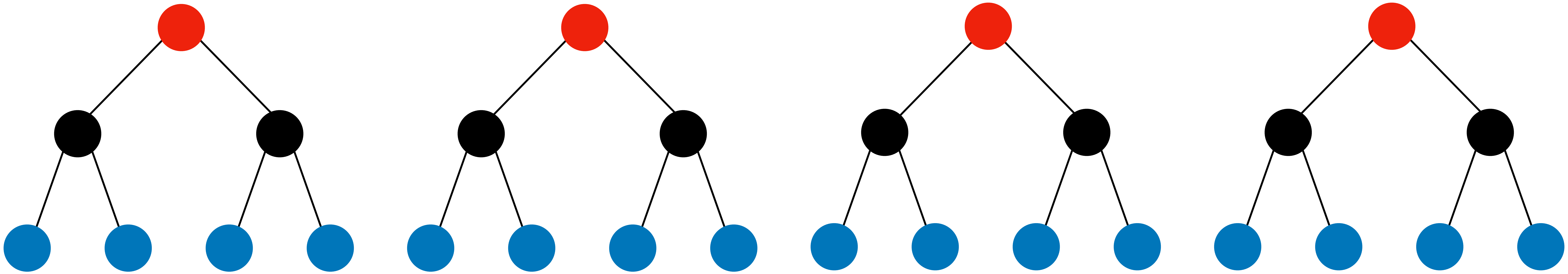
Arbre GGM (Goldreich, Goldwasser, Micali)

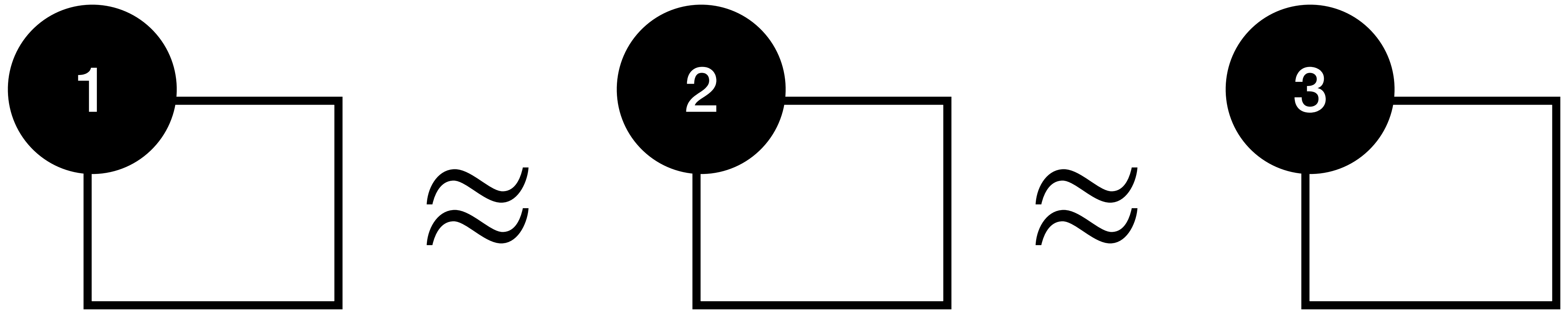




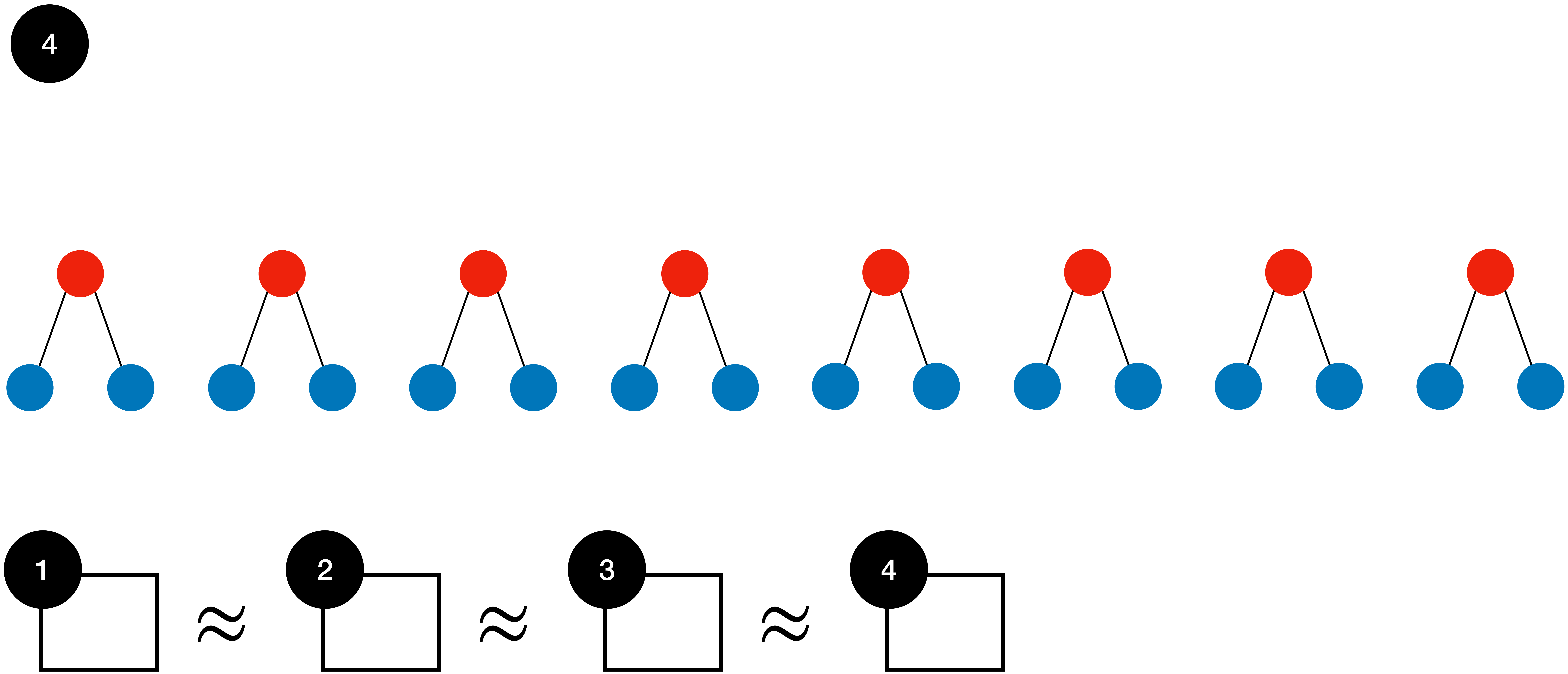
Arbre GGM (Goldreich, Goldwasser, Micali)

3

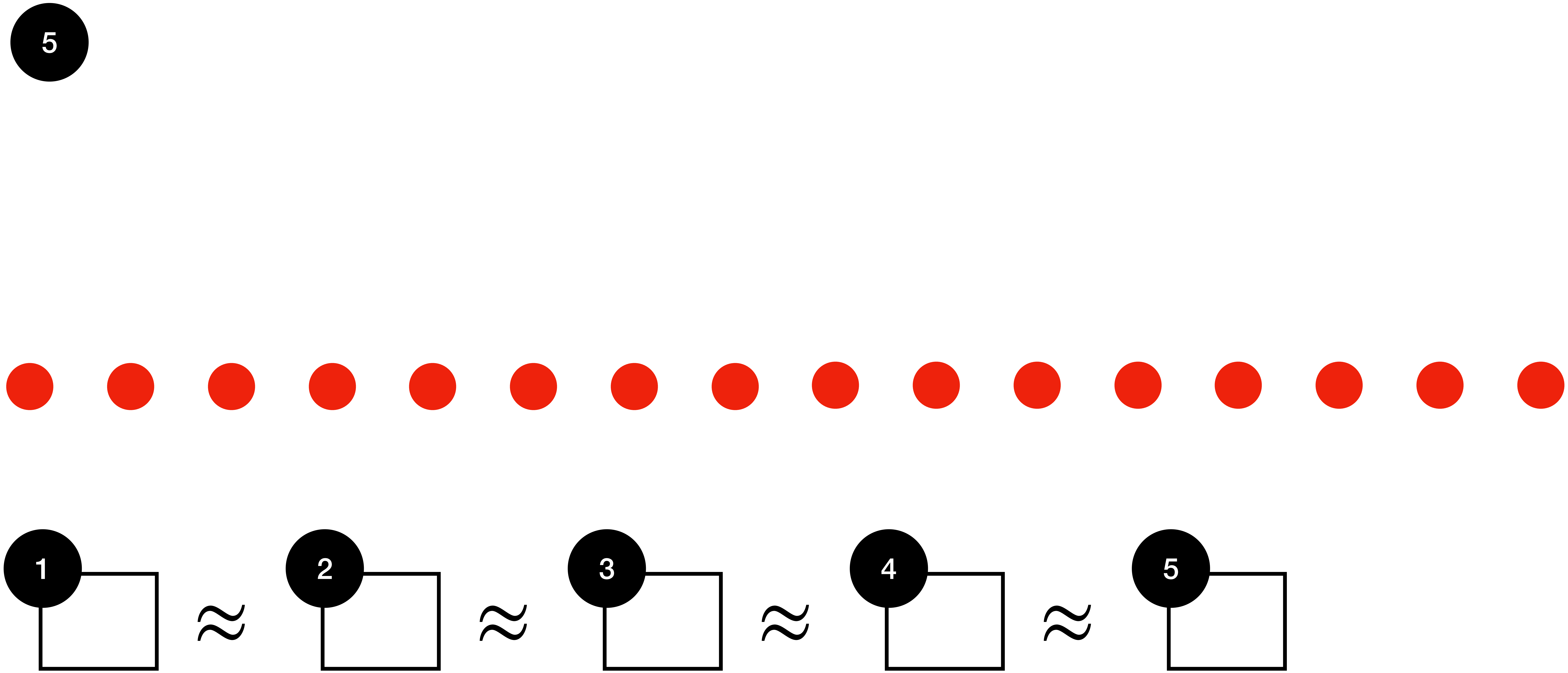




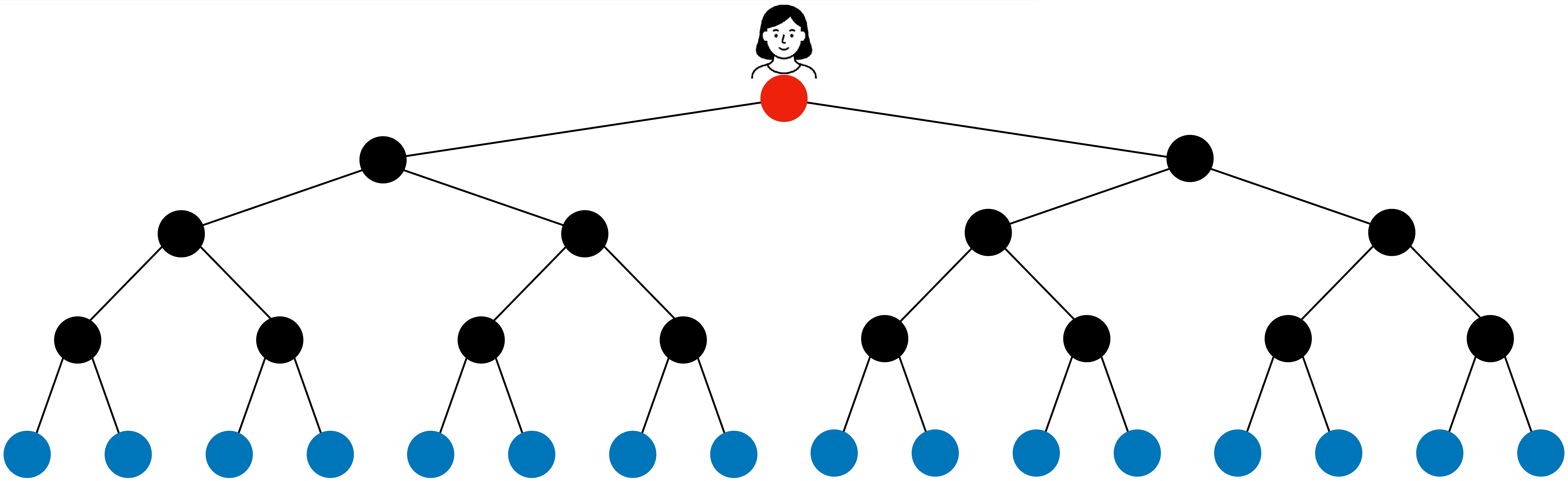
Arbre GGM (Goldreich, Goldwasser, Micali)



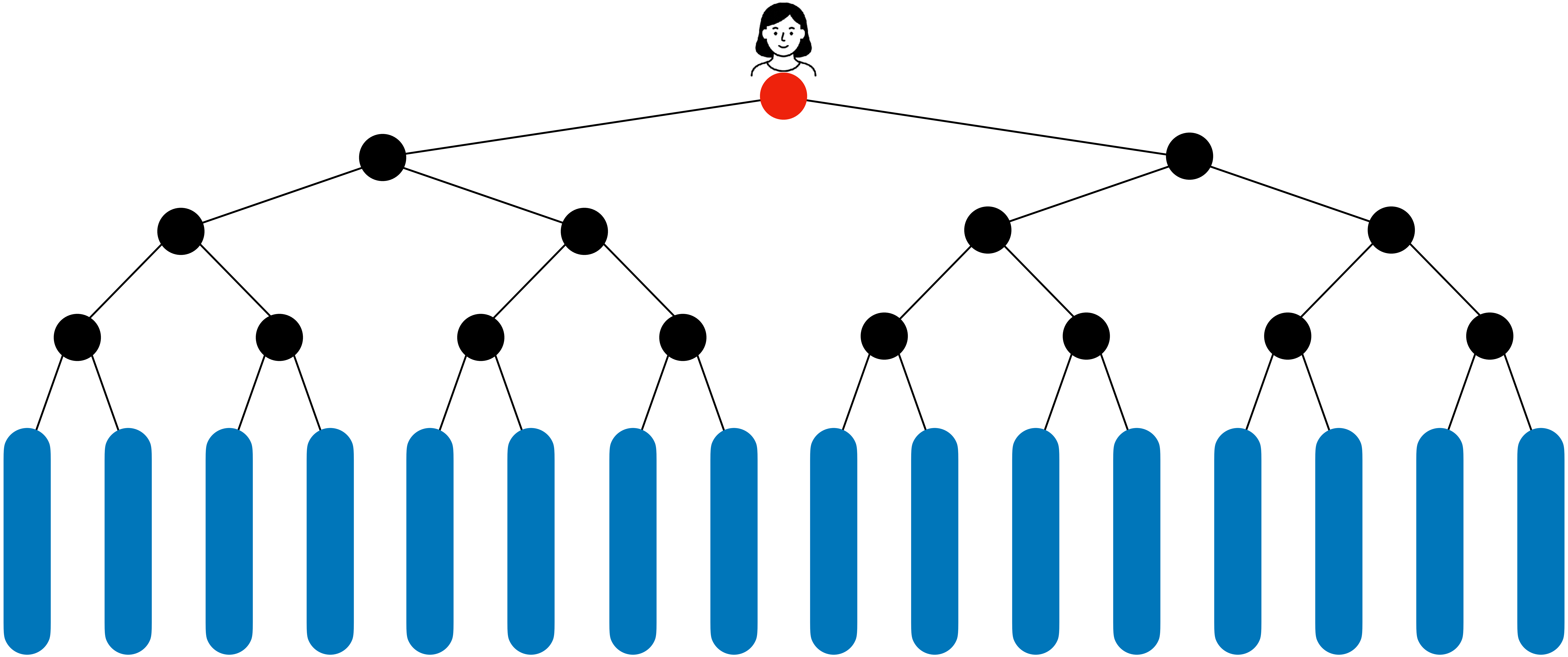
Arbre GGM (Goldreich, Goldwasser, Micali)



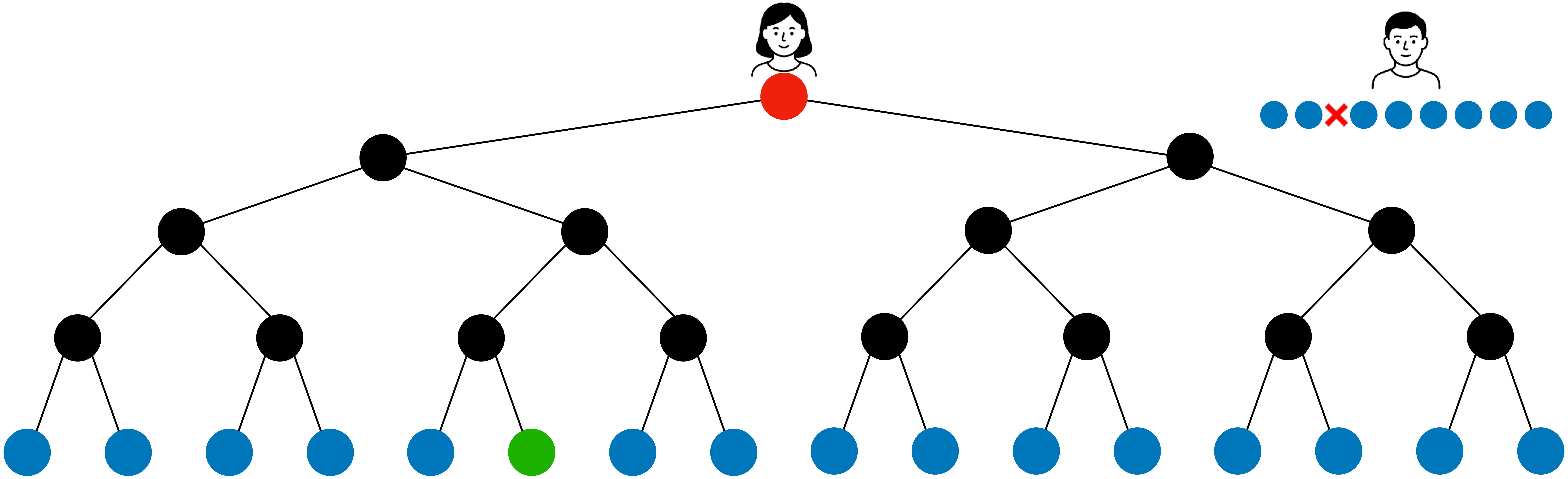
Arbre GGM (Goldreich, Goldwasser, Micali)



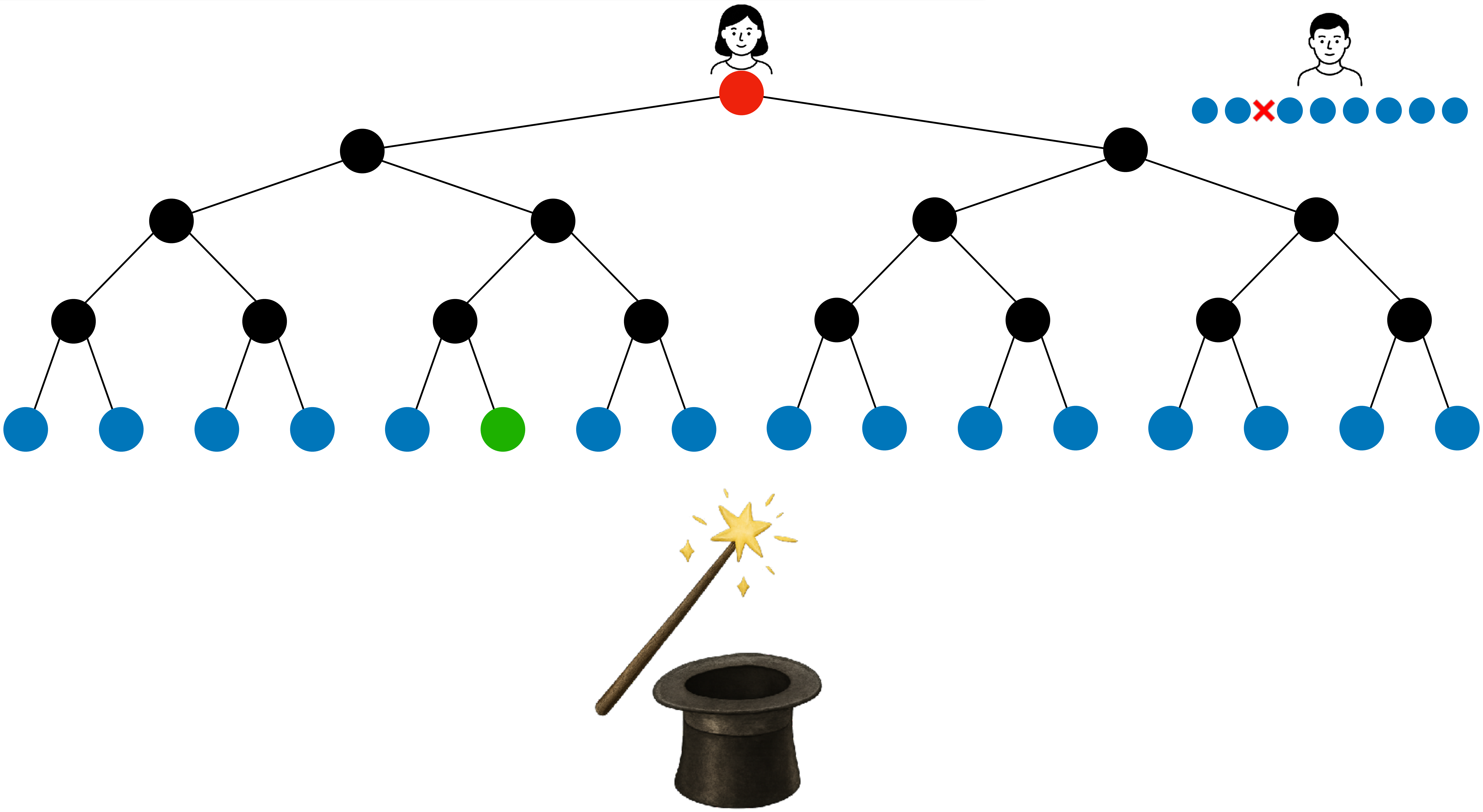
Arbre GGM + chiffrement par flot



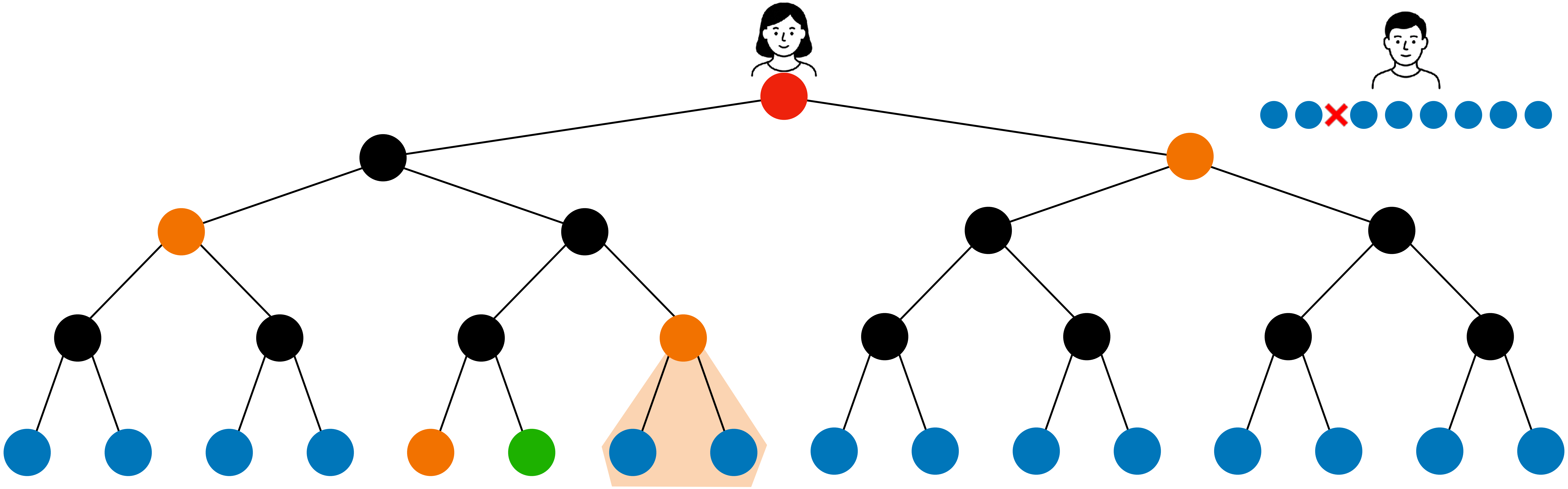
Le protocole SoftSpokenOT (Roy, Crypto'22)



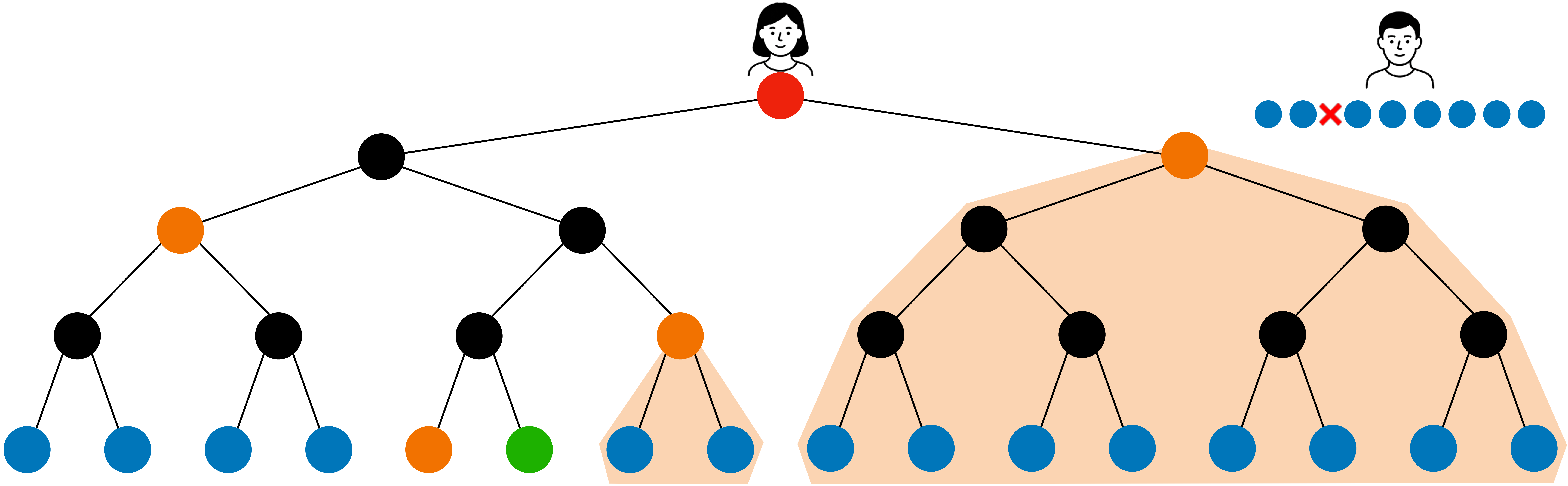
Le protocole SoftSpokenOT (Roy, Crypto'22)



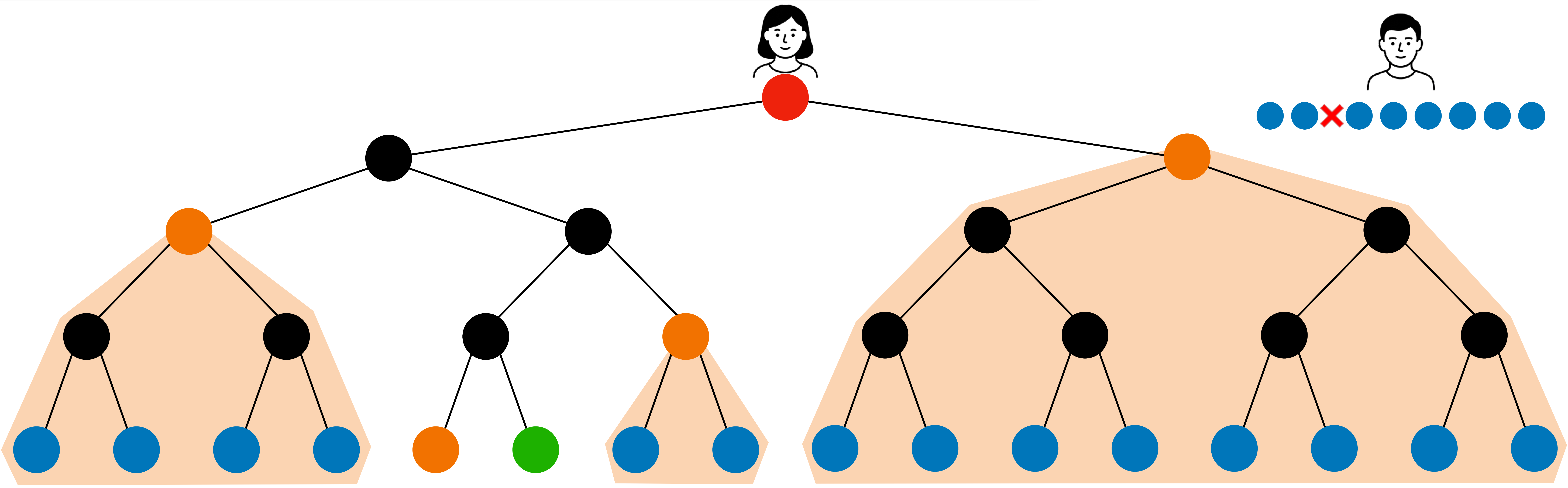
Partager toutes les feuilles sauf une



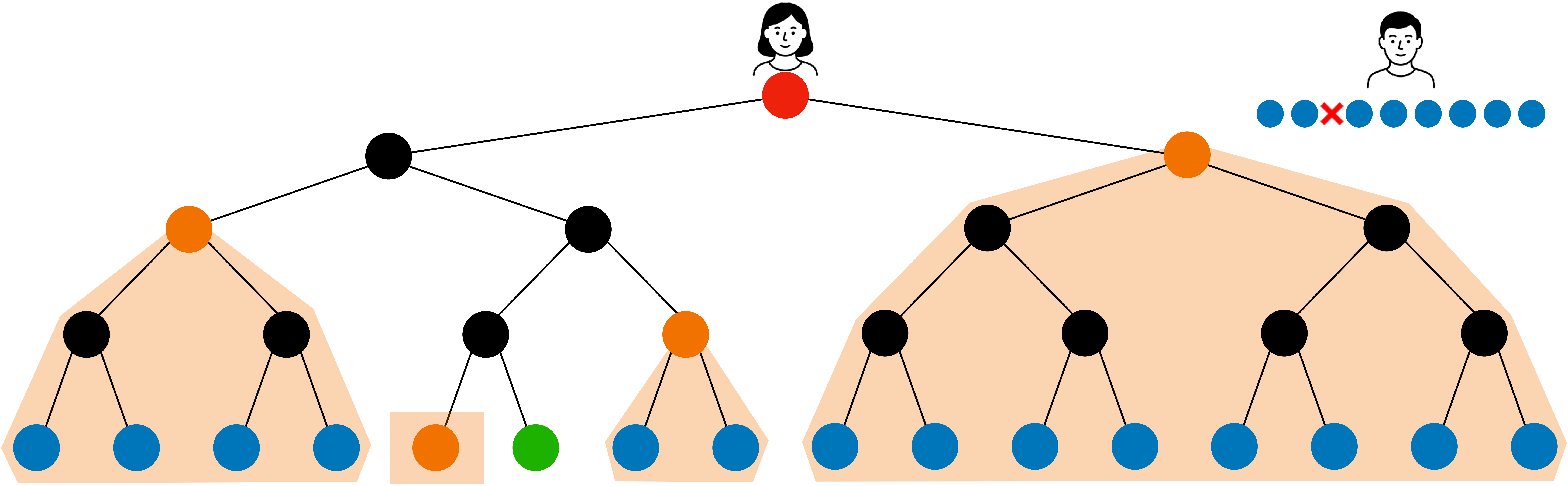
Partager toutes les feuilles sauf une



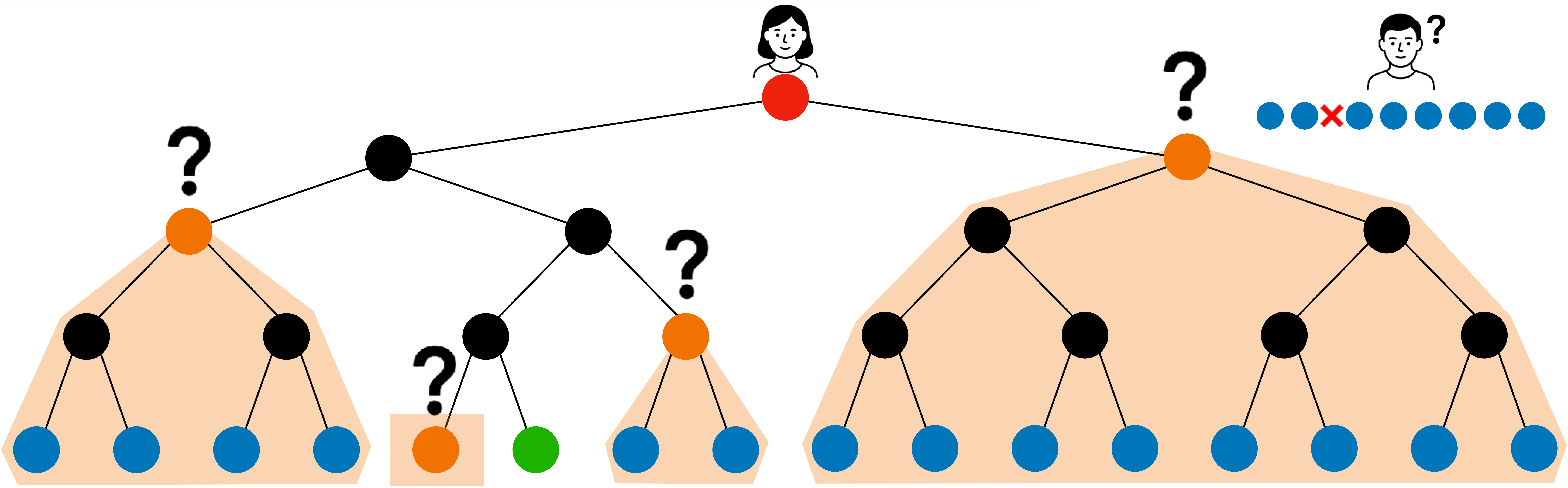
Partager toutes les feuilles sauf une



Partager toutes les feuilles sauf une



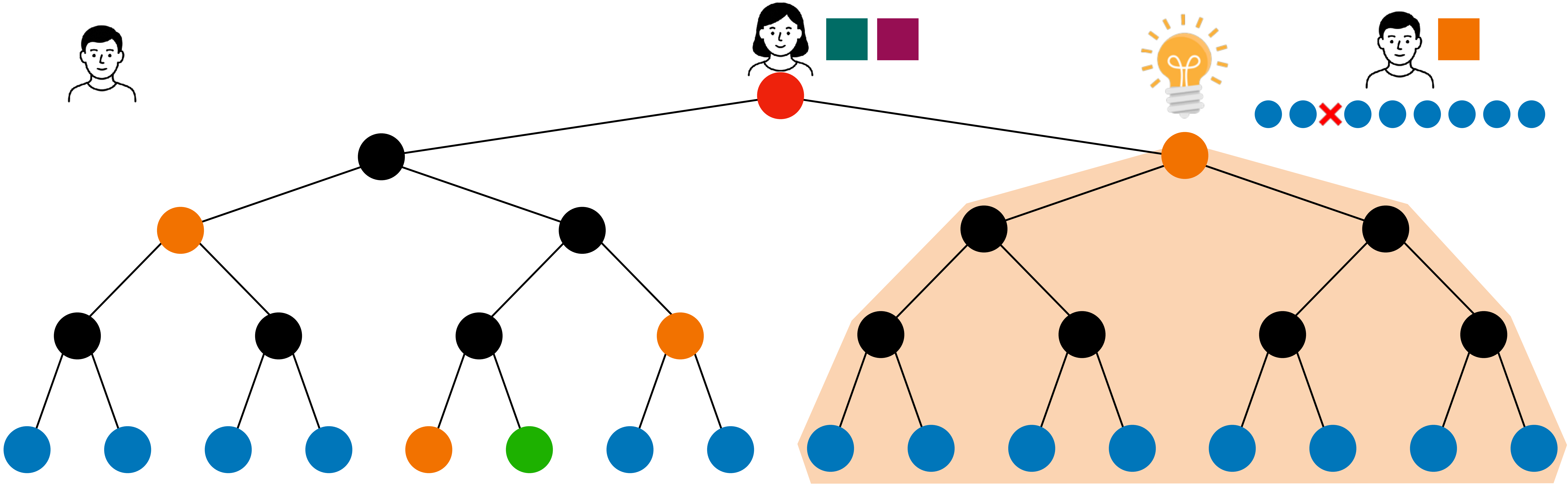
Partager toutes les feuilles sauf une



Partager toutes les feuilles sauf une

Partager toutes les feuilles sauf une

Partager toutes les feuilles sauf une



Partager toutes les feuilles sauf une

Partager toutes les feuilles sauf une

Partager toutes les feuilles sauf une

Partager toutes les feuilles sauf une

Partager toutes les feuilles sauf une

Partager toutes les feuilles sauf une

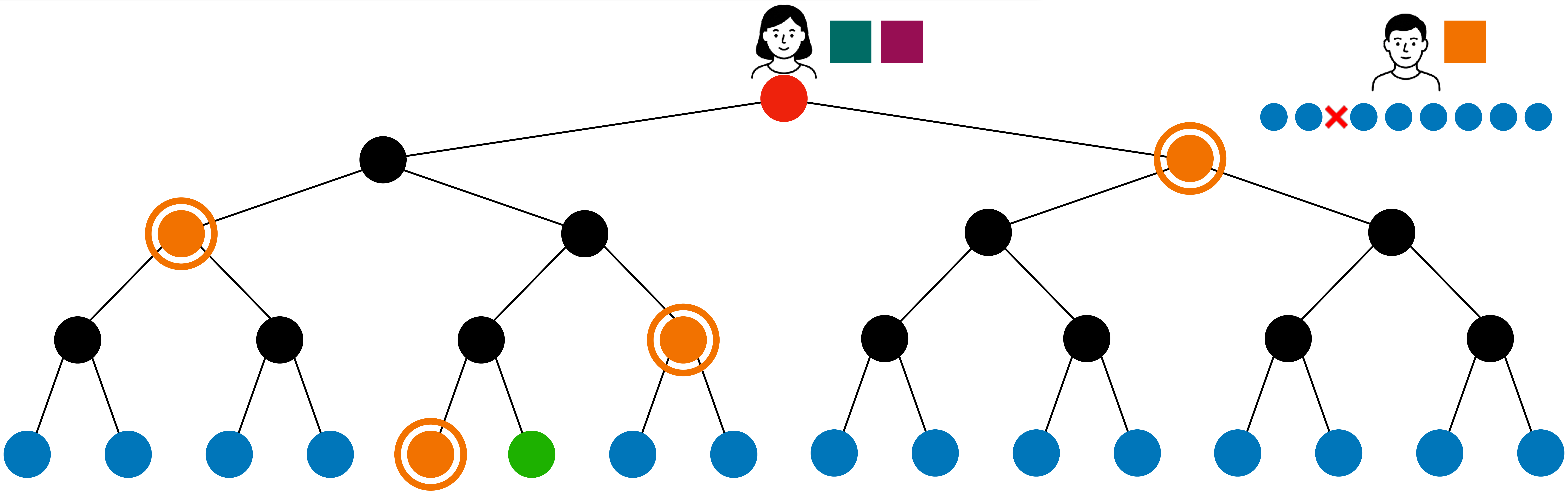
Partager toutes les feuilles sauf une

Partager toutes les feuilles sauf une

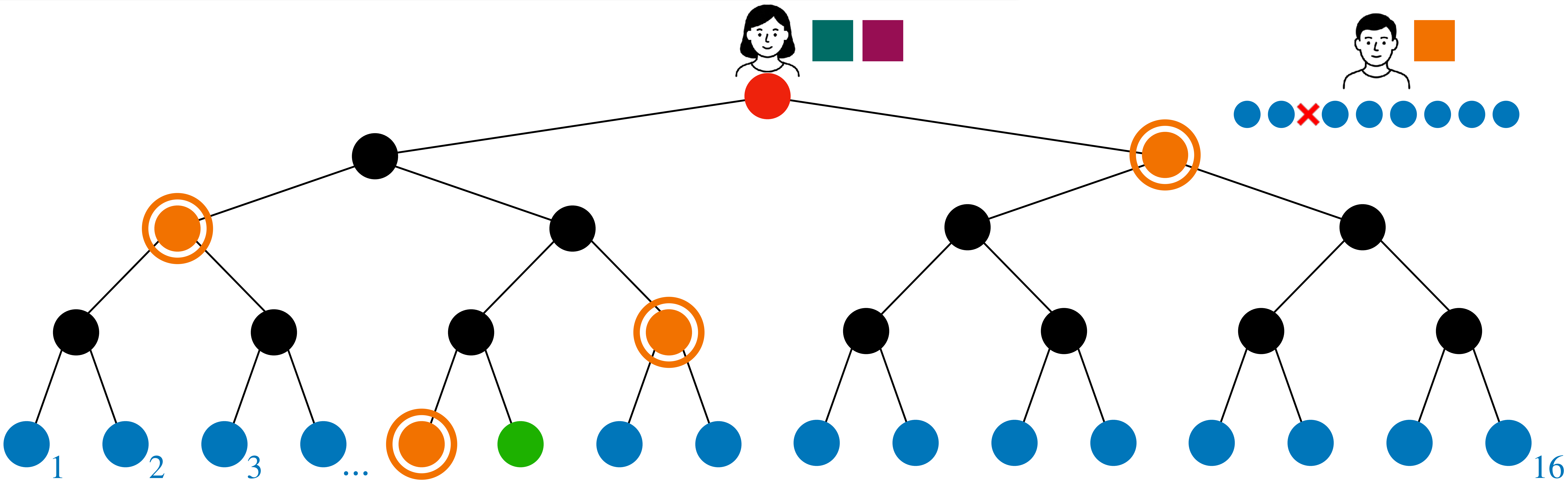
Partager toutes les feuilles sauf une

S'il y a n feuilles, on a utilisé $\log n$ transfers inconscients

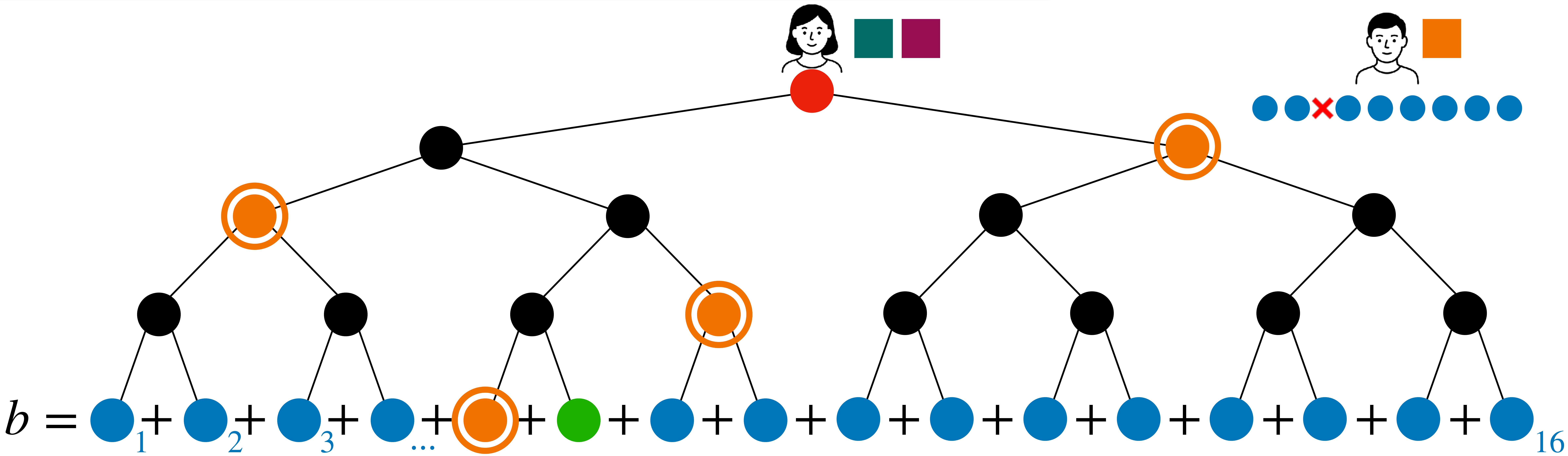
Retour aux transferts inconscients corrélés



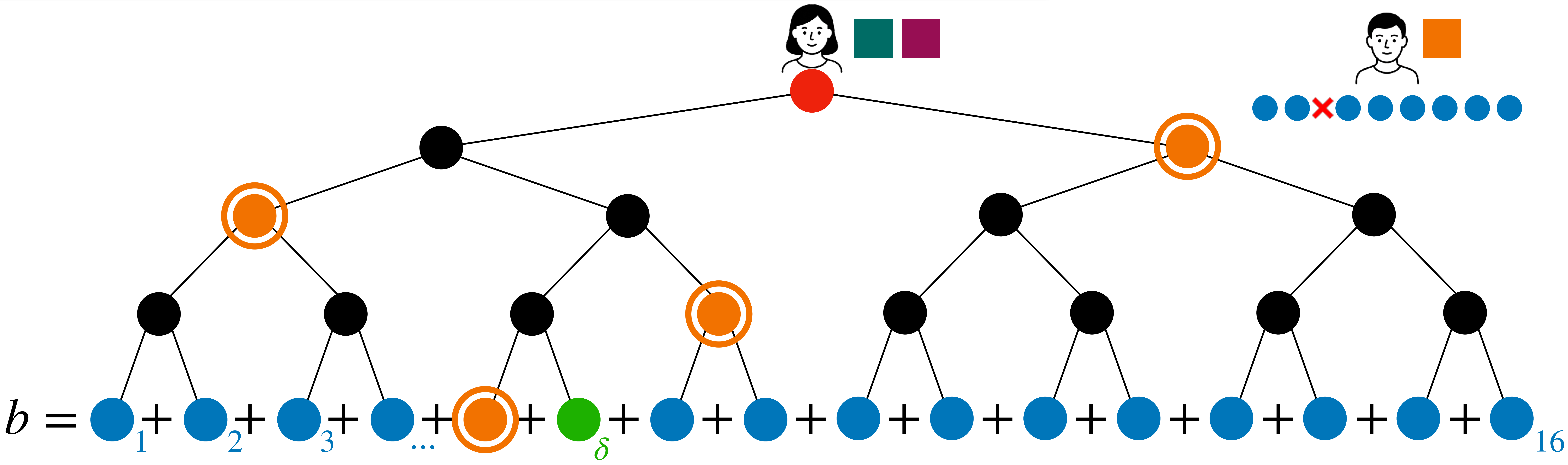
Retour aux transferts inconscients corrélés



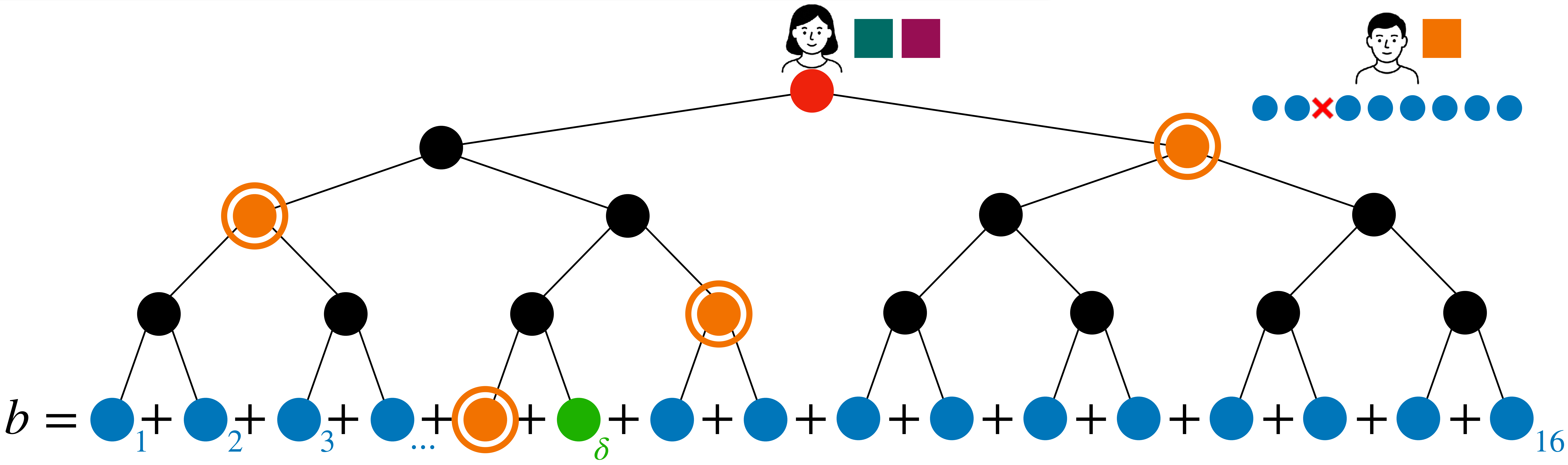
Retour aux transferts inconscients corrélés



Retour aux transferts inconscients corrélés

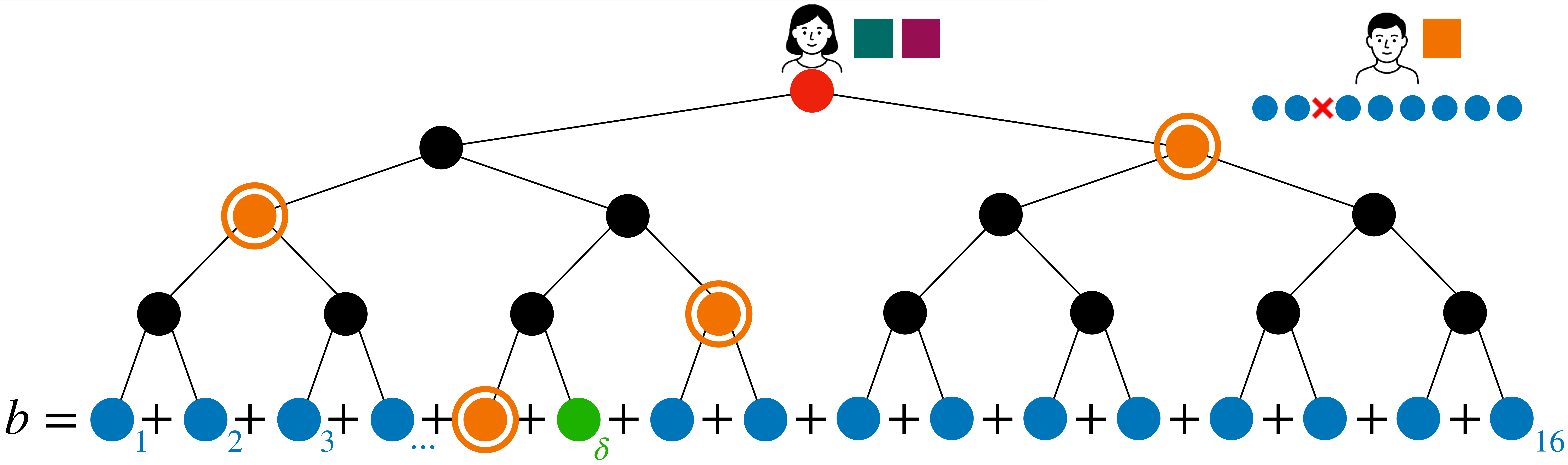


Retour aux transferts inconscients corrélés



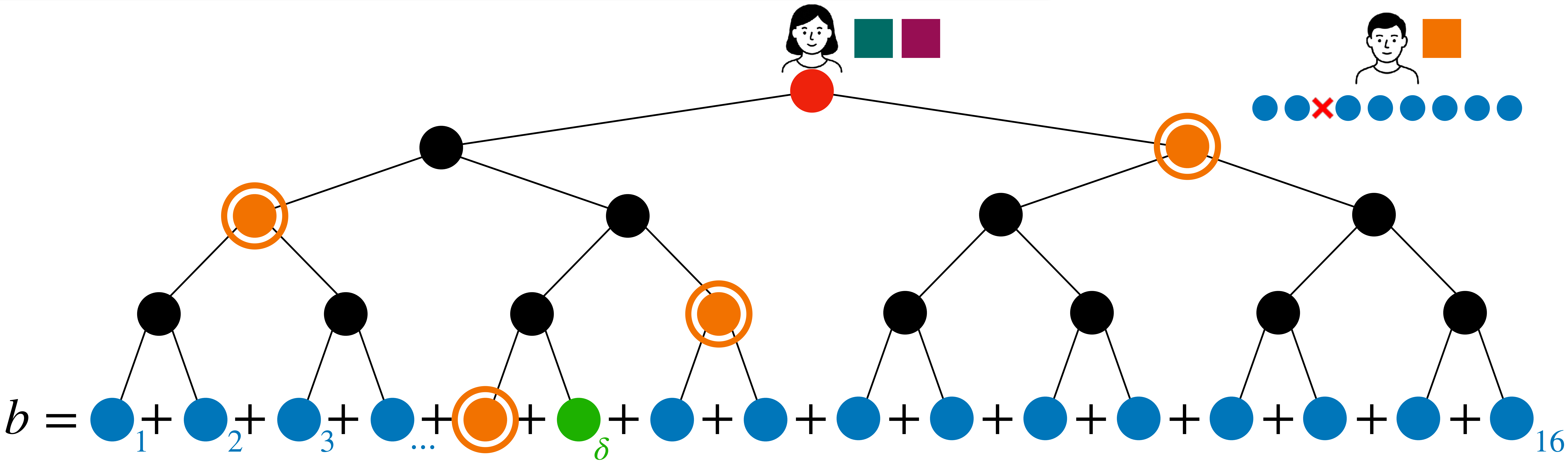
$$\sum_{i=1}^{16} i \cdot \bullet_i + \sum_{i=1}^{16} (\delta - i) \cdot \bullet_i = \delta \cdot \sum_{i=1}^{16} \bullet_i = b \cdot \delta$$

Retour aux transferts inconscients corrélés



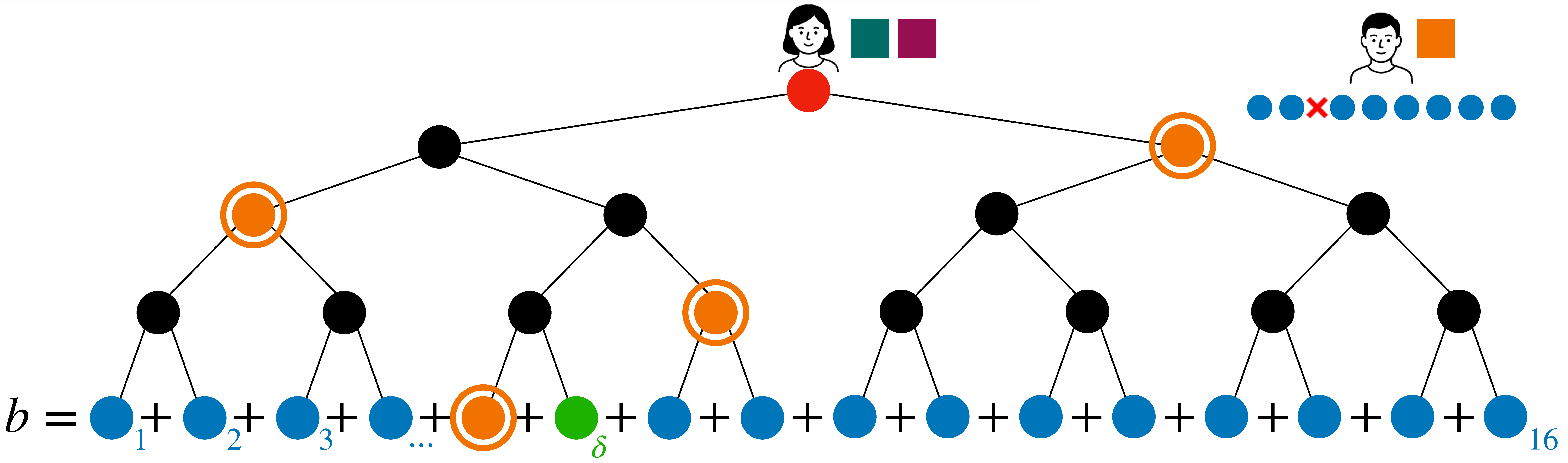
$$\boxed{\sum_{i=1}^{16} i \cdot \bullet_i} + \sum_{i=1}^{16} (\delta - i) \cdot \bullet_i = \delta \cdot \sum_{i=1}^{16} \bullet_i = b \cdot \delta$$

Retour aux transferts inconscients corrélés



$$\boxed{\sum_{i=1}^{16} i \cdot \bullet_i} + \boxed{\sum_{i=1}^{16} (\delta - i) \cdot \bullet_i} = \delta \cdot \sum_{i=1}^{16} \bullet_i = b \cdot \delta$$

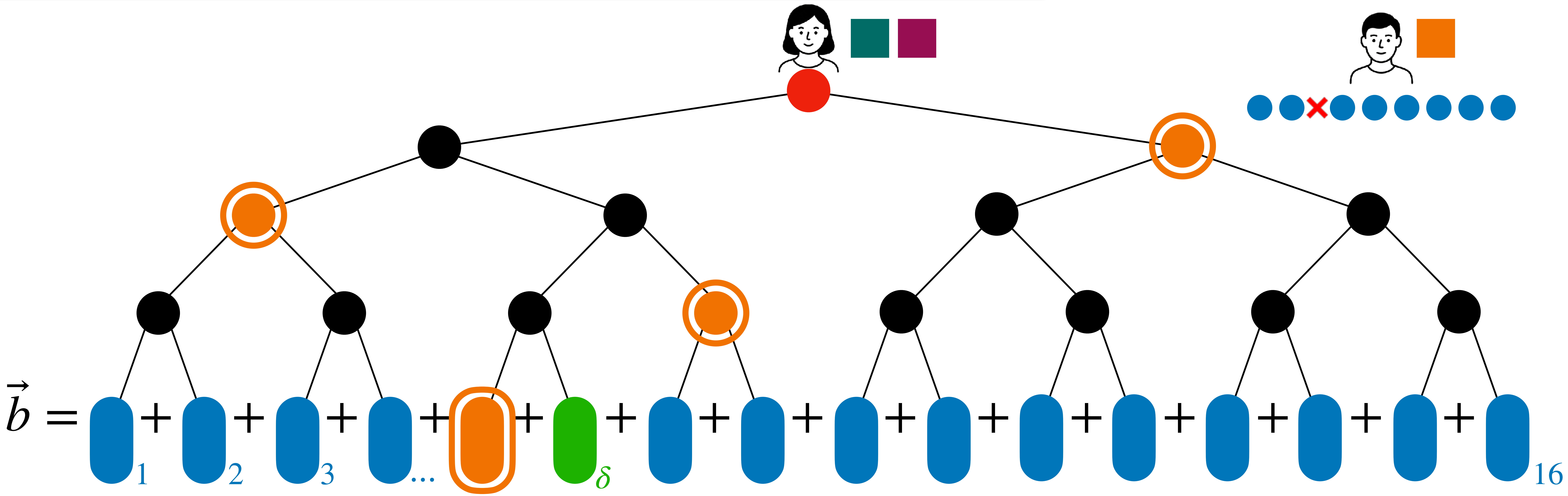
Retour aux transferts inconscients corrélés



$$\underbrace{\boxed{\sum_{i=1}^{16} i \cdot \bullet_i}} + \boxed{\sum_{i=1}^{16} (\delta - i) \cdot \bullet_i} = \delta \cdot \sum_{i=1}^{16} \bullet_i = b \cdot \delta$$

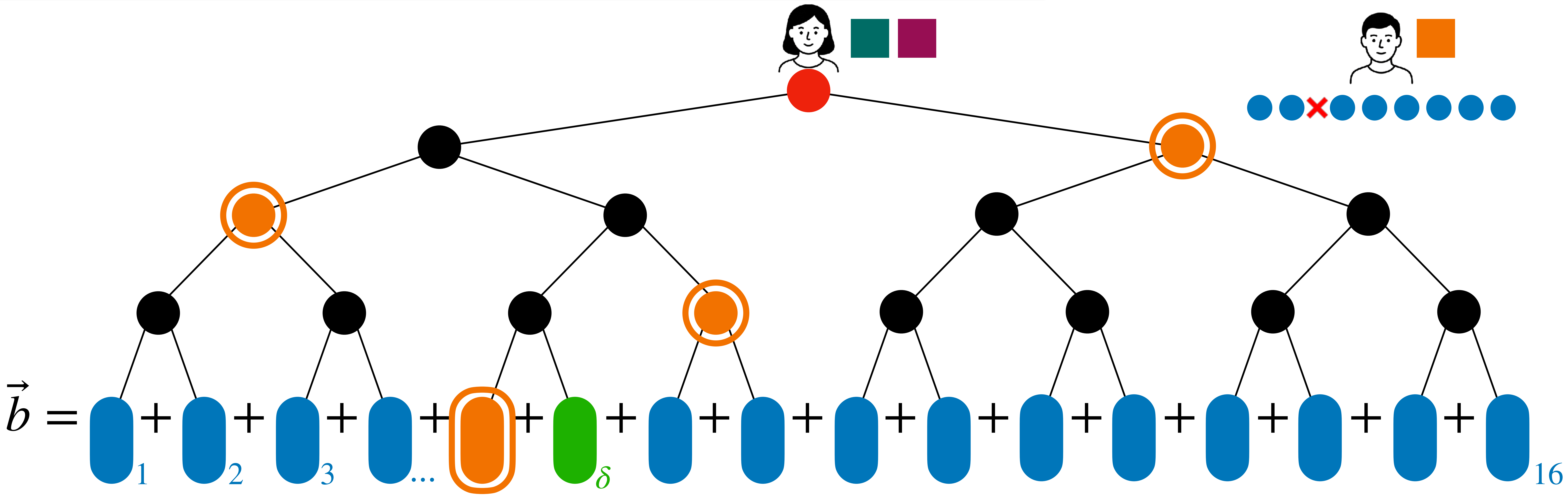
$$(\delta - \delta) \cdot \bullet_\delta = 0$$

Retour aux transferts inconscients corrélés



$$\boxed{\sum_{i=1}^{16} i \cdot \bullet_i} + \boxed{\sum_{i=1}^{16} (\delta - i) \cdot \bullet_i} = \delta \cdot \sum_{i=1}^{16} \bullet_i = \vec{b} \cdot \delta$$

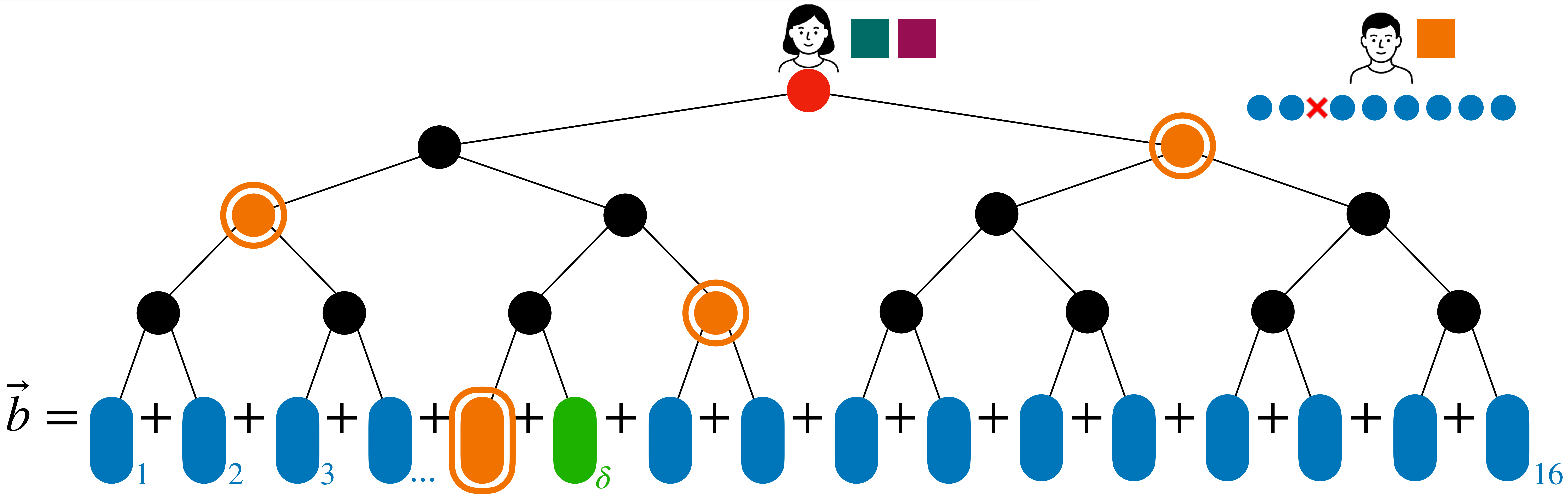
Retour aux transferts inconscients corrélés



$$\boxed{\sum_{i=1}^{16} i \cdot \bullet_i} + \boxed{\sum_{i=1}^{16} (\delta - i) \cdot \bullet_i} = \delta \cdot \sum_{i=1}^{16} \bullet_i = \vec{b} \cdot \delta$$

$-\vec{u}$

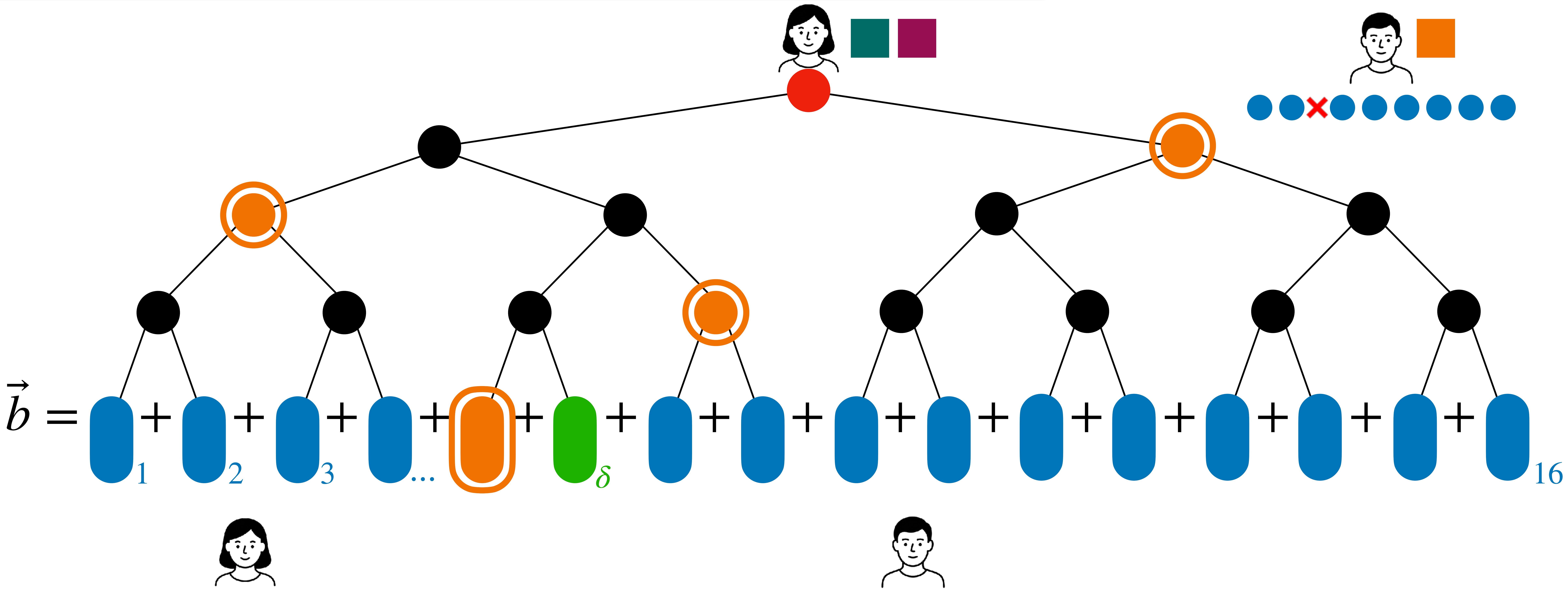
Retour aux transferts inconscients corrélés



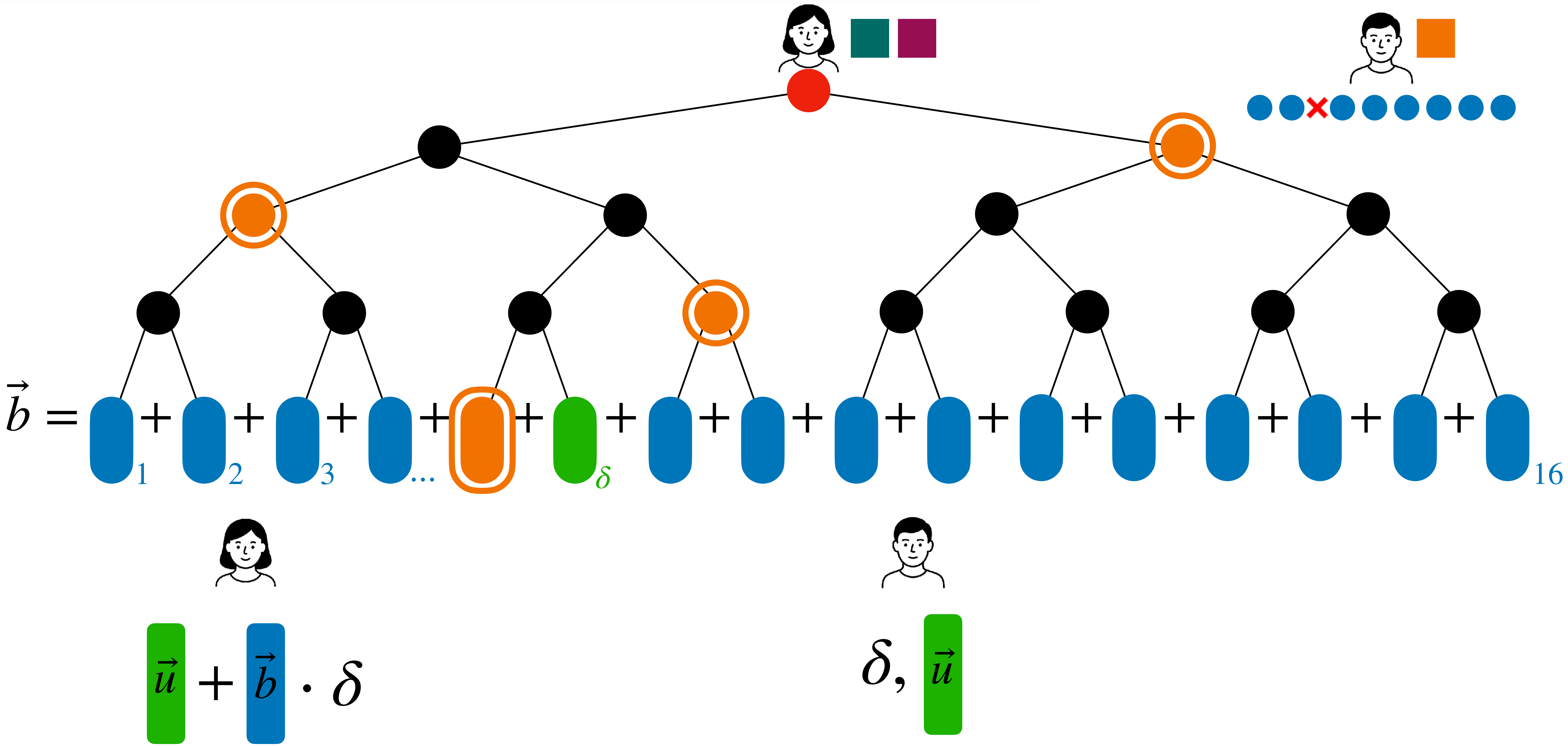
$$\boxed{\sum_{i=1}^{16} i \cdot \bullet_i} + \boxed{\sum_{i=1}^{16} (\delta - i) \cdot \bullet_i} = \delta \cdot \sum_{i=1}^{16} \bullet_i = \vec{b} \cdot \delta$$

$\vec{b} \cdot \delta + \vec{u}$ $\quad$ $-\vec{u}$

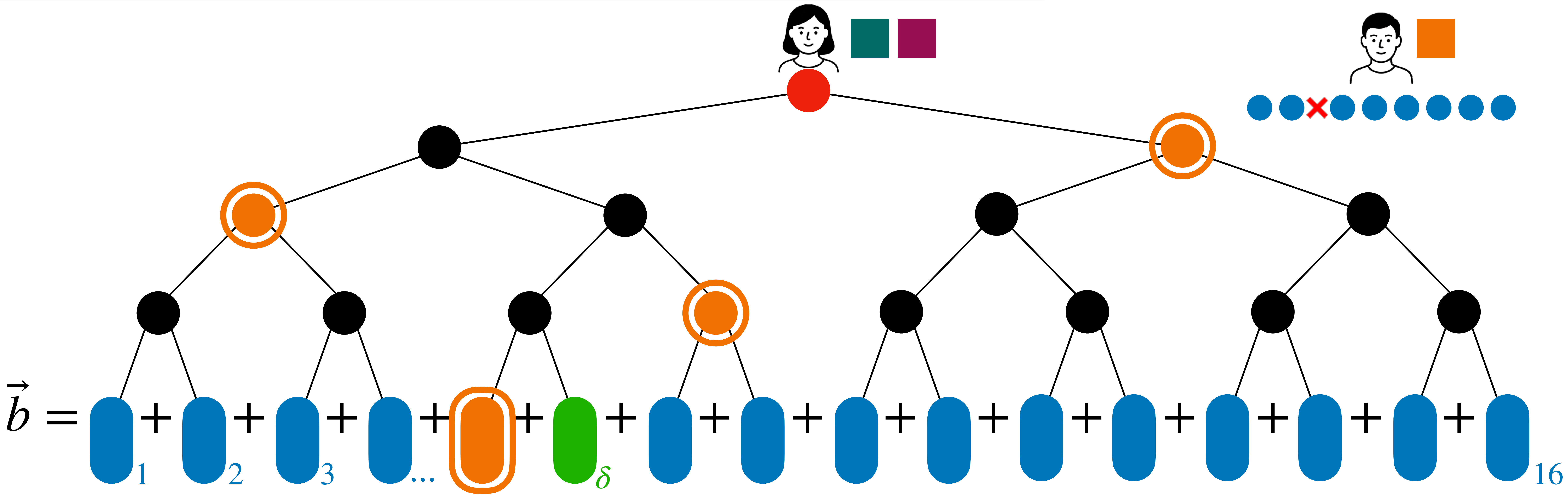
Retour aux transferts inconscients corrélés



Retour aux transferts inconscients corrélés

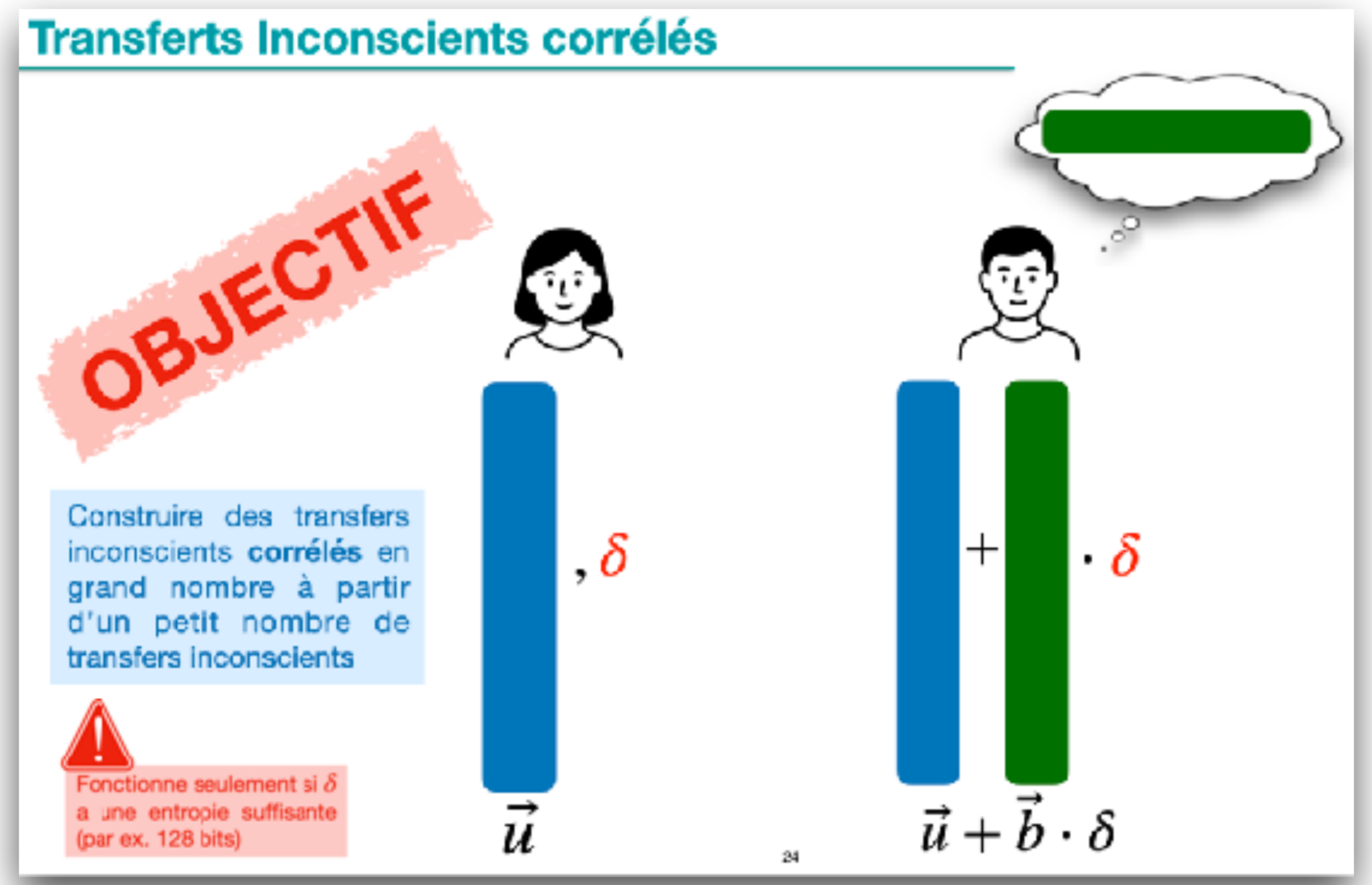


Retour aux transferts inconscients corrélés

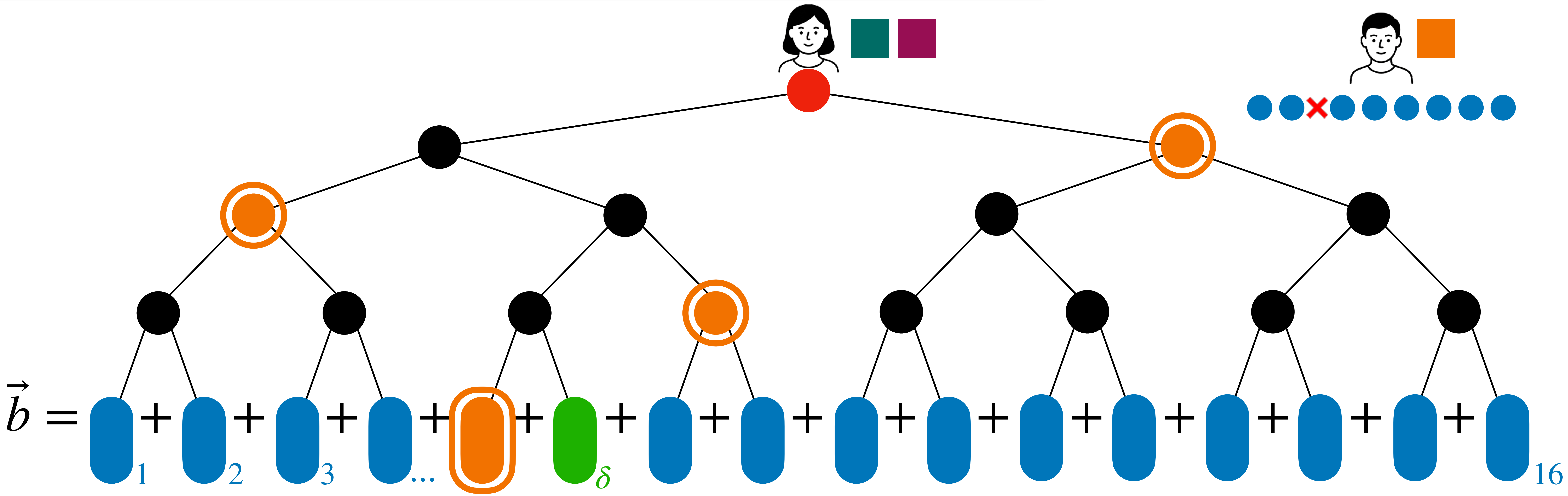


$\vec{u} + \vec{b} \cdot \delta$

$\delta, \vec{u}$



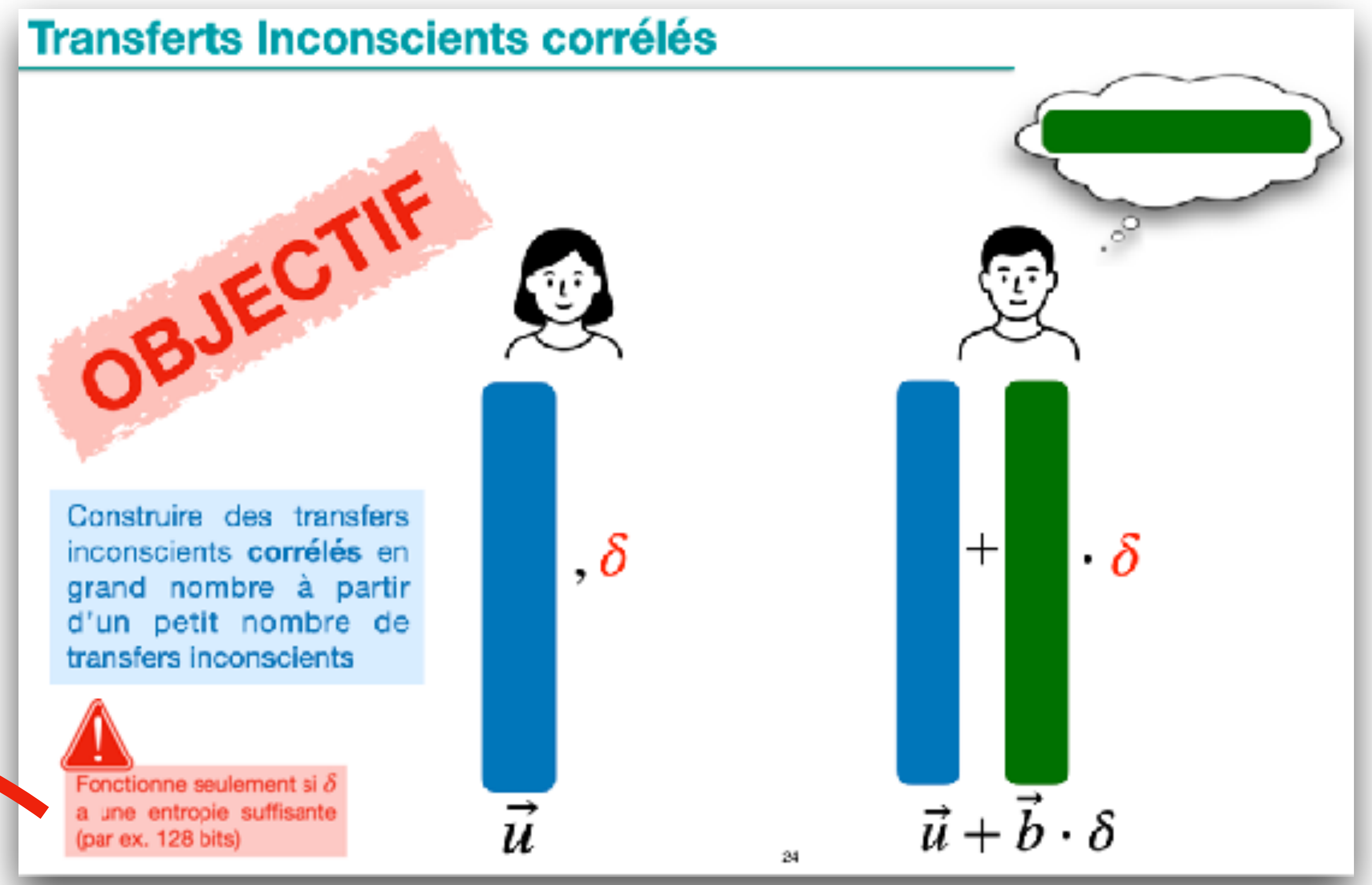
Retour aux transferts inconscients corrélés



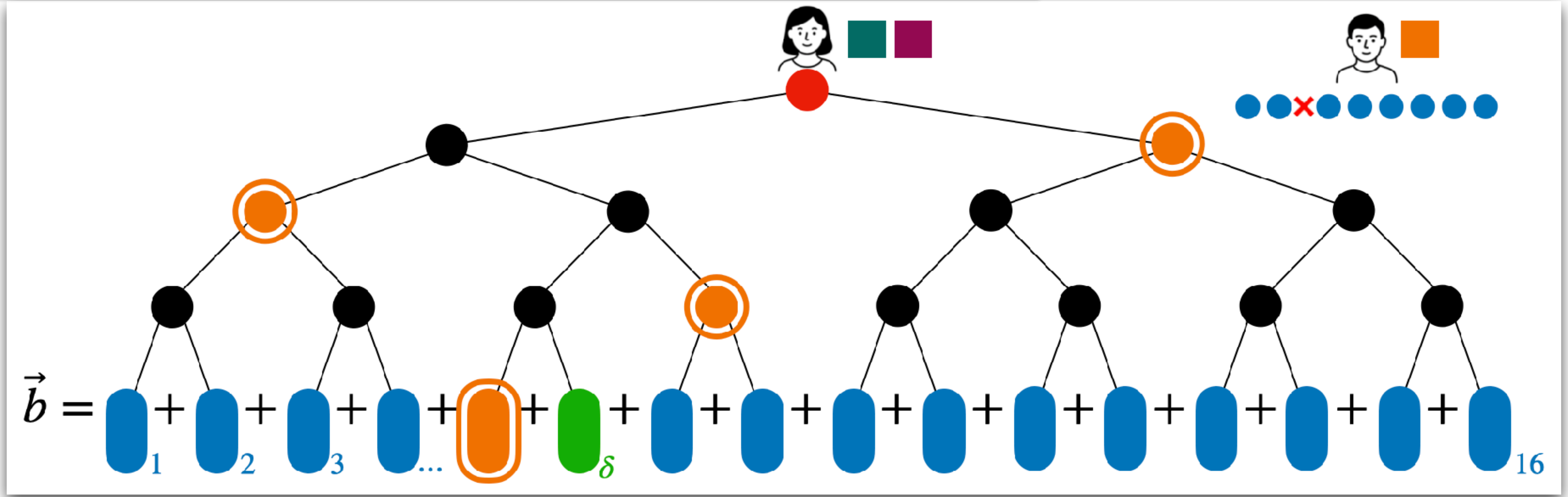
$\vec{u} + \vec{b} \cdot \delta$

Fonctionne seulement si δ a une entropie suffisante (par ex. 128 bits)

$\delta, \vec{u}$



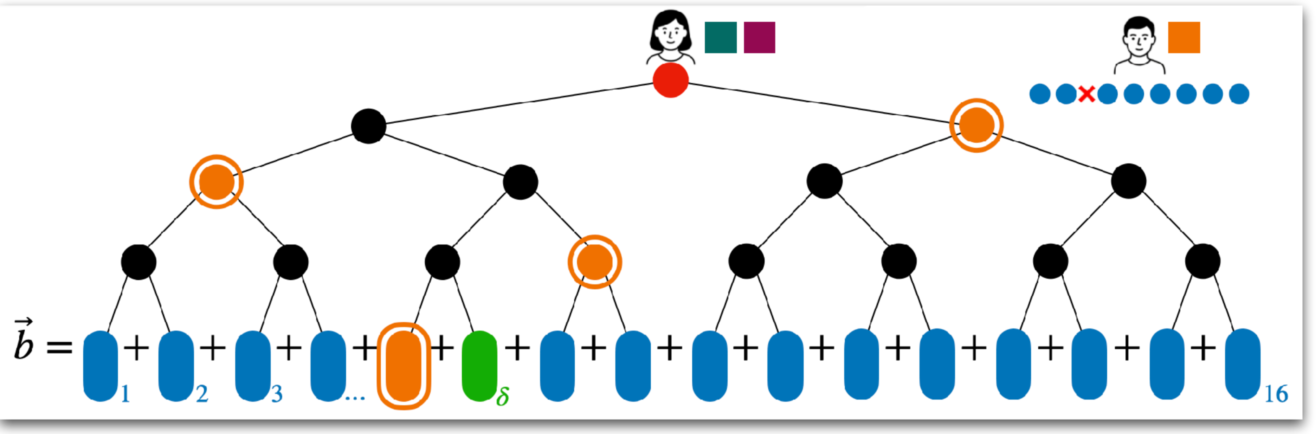
Retour aux transferts inconscients corrélés



$$\vec{u} + \vec{b} \cdot \delta$$

$$\delta, \vec{u}$$

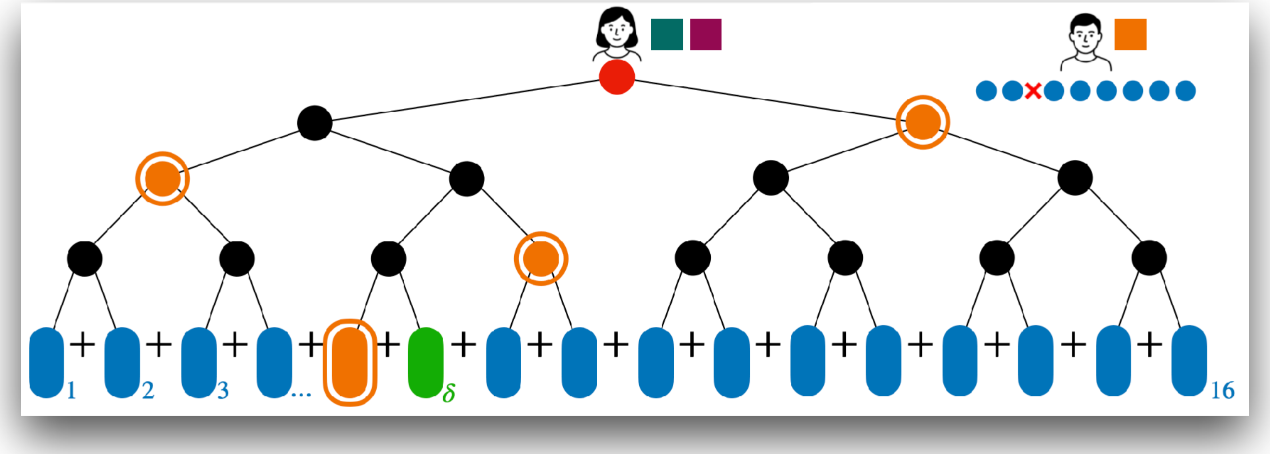
Retour aux transferts inconscients corrélés



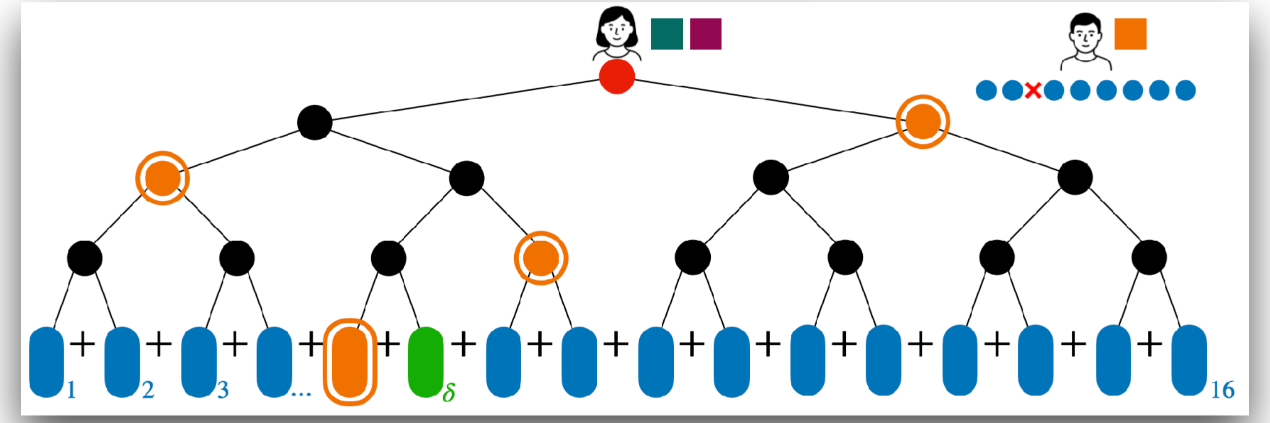
$$\vec{u} + \vec{b} \cdot \delta$$

$$\delta, \vec{u}$$

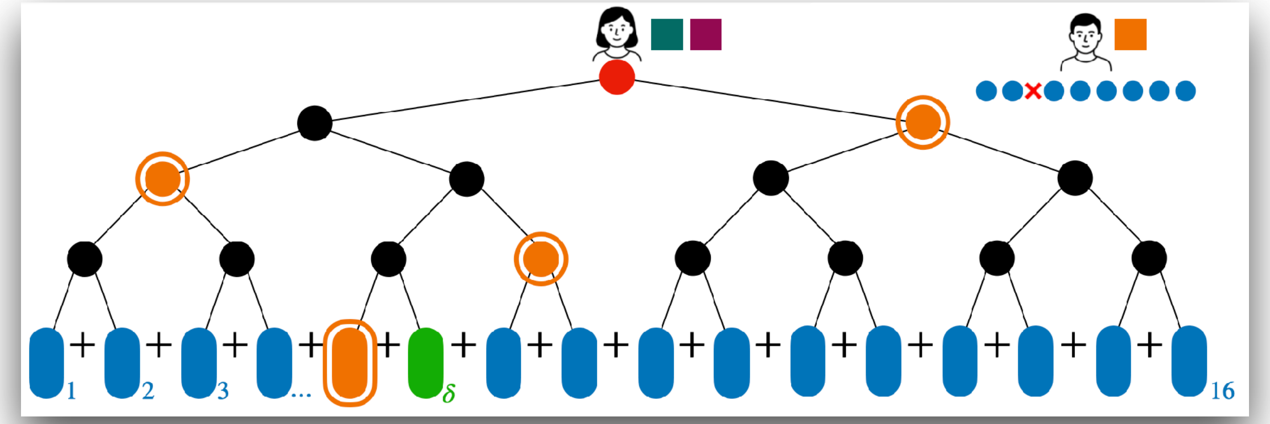
Retour aux transferts inconscients corrélés



Retour aux transferts inconscients corrélés



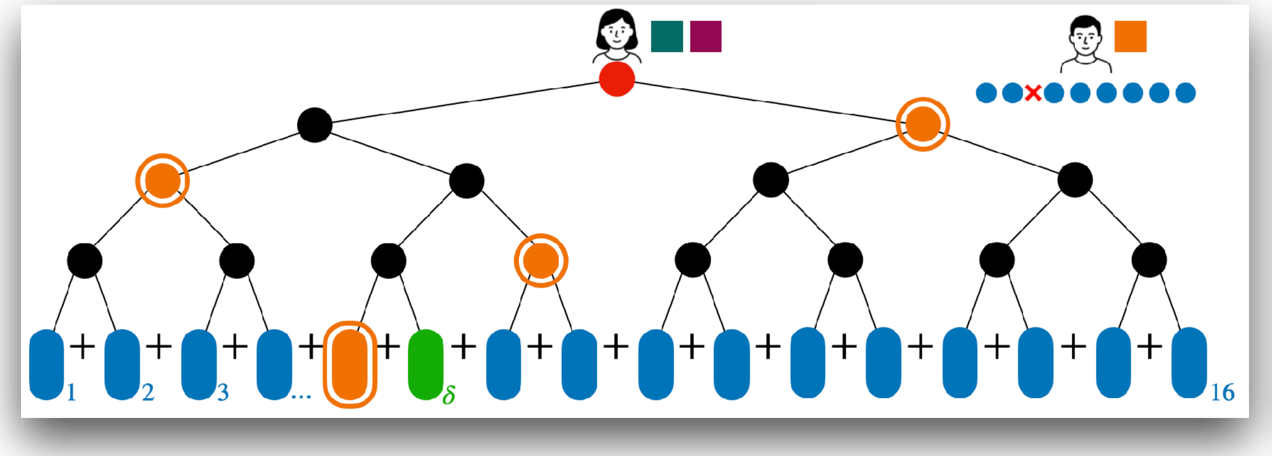
Retour aux transferts inconscients corrélés

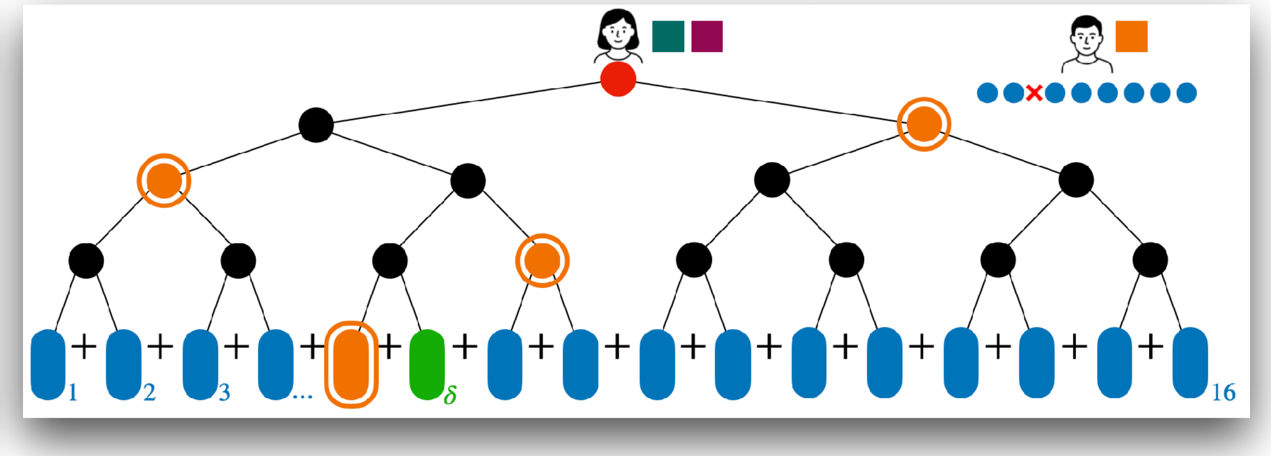


$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1$$

$$\delta_1, \vec{u}_1$$

Retour aux transferts inconscients corrélés

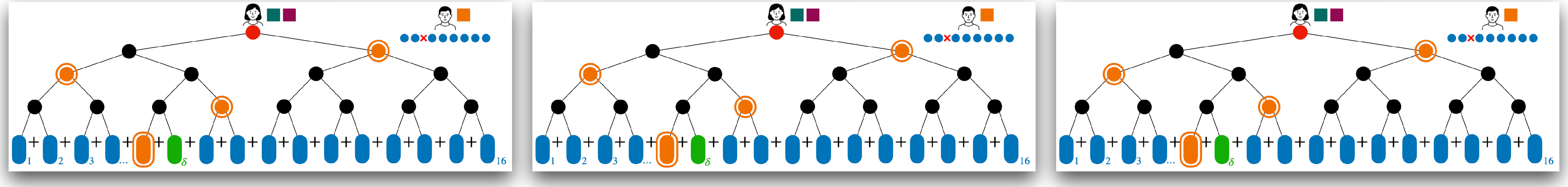




$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1$$
$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2$$

$$\delta_1, \vec{u}_1$$
$$\delta_2, \vec{u}_2$$

Retour aux transferts inconscients corrélés

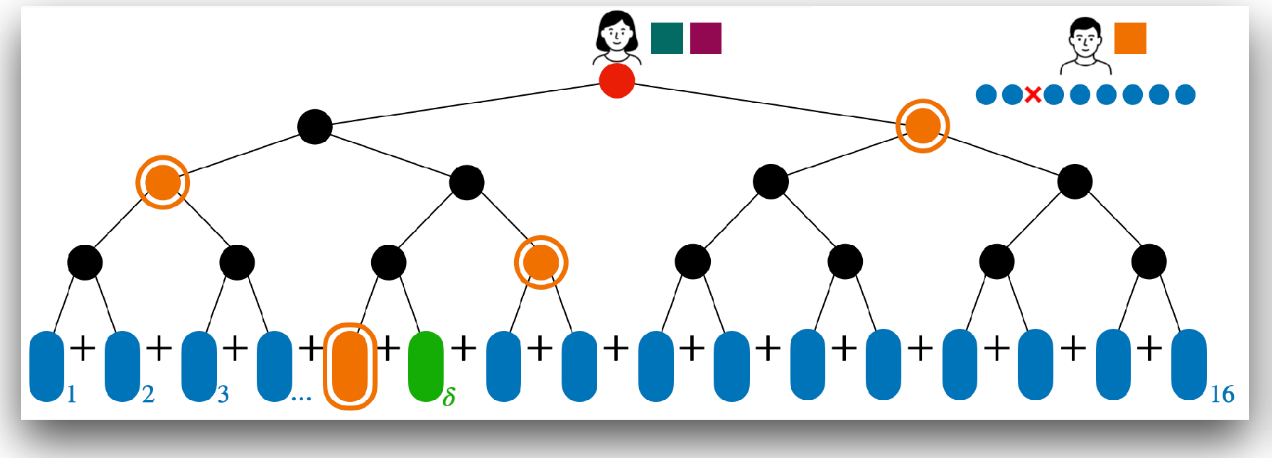
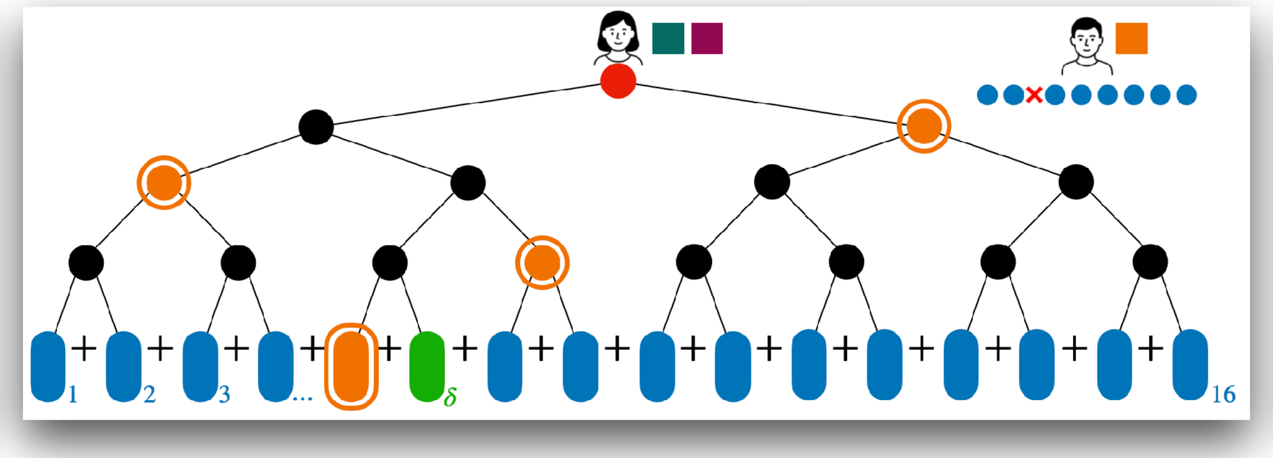
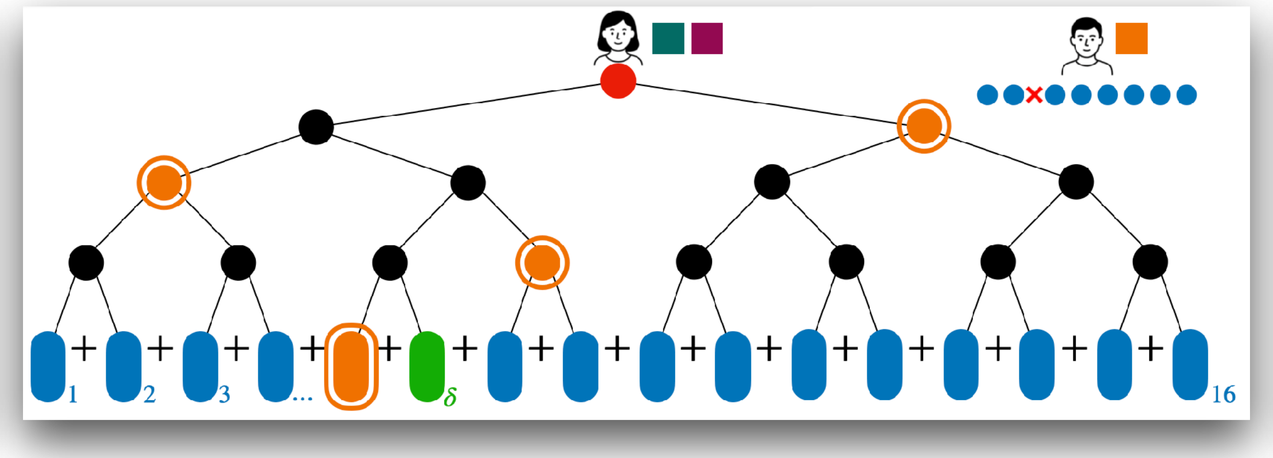
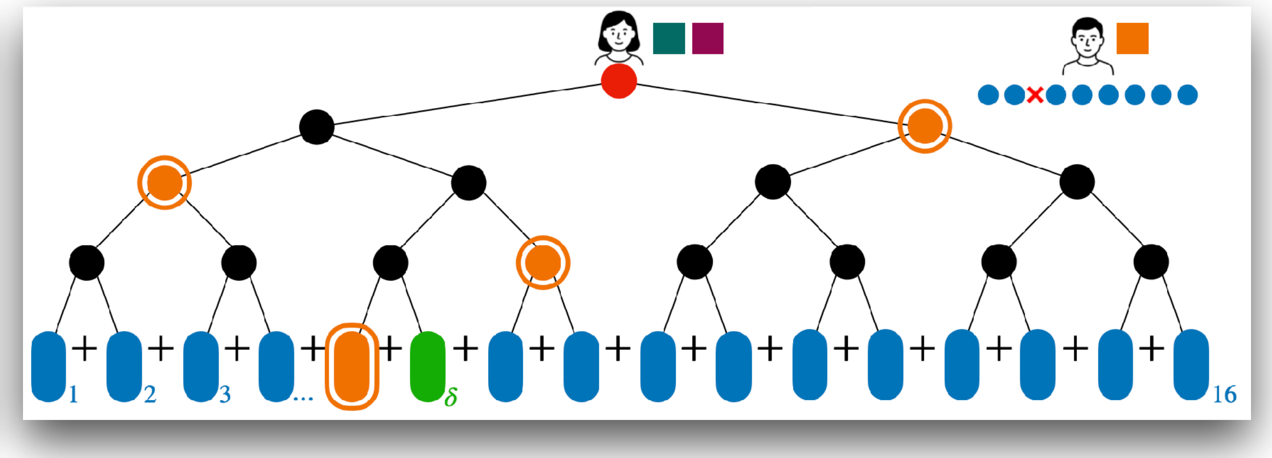


$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1 \qquad \delta_1, \vec{u}_1$$

$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2 \qquad \delta_2, \vec{u}_2$$

$$\vec{u}_3 + \vec{b}_3 \cdot \delta_3 \qquad \delta_3, \vec{u}_3$$

Retour aux transferts inconscients corrélés

$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1$$
$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2$$
$$\vec{u}_3 + \vec{b}_3 \cdot \delta_3$$
$$\vec{u}_4 + \vec{b}_4 \cdot \delta_4$$

$$\delta_1, \vec{u}_1$$
$$\delta_2, \vec{u}_2$$
$$\delta_3, \vec{u}_3$$
$$\delta_4, \vec{u}_4$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$\vec{u}_1 + \vec{b}_1 \cdot \delta_1$	$\delta_1, \vec{u}_1$
$\vec{u}_2 + \vec{b}_2 \cdot \delta_2$	$\delta_2, \vec{u}_2$
$\vec{u}_3 + \vec{b}_3 \cdot \delta_3$	$\delta_3, \vec{u}_3$
$\vec{u}_4 + \vec{b}_4 \cdot \delta_4$	$\delta_4, \vec{u}_4$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

Les b_i ne se factorisent pas : on ne peut pas faire de combinaison linéaire

$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1$$
$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2$$
$$\vec{u}_3 + \vec{b}_3 \cdot \delta_3$$
$$\vec{u}_4 + \vec{b}_4 \cdot \delta_4$$

$$\delta_1, \vec{u}_1$$
$$\delta_2, \vec{u}_2$$
$$\delta_3, \vec{u}_3$$
$$\delta_4, \vec{u}_4$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

Les b_i ne se factorisent pas : on ne peut pas faire de combinaison linéaire

On va envoyer des correctifs pour rendre les $\vec{b}_i$ égaux

$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1 \qquad \delta_1, \vec{u}_1$$
$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2 \qquad \delta_2, \vec{u}_2$$
$$\vec{u}_3 + \vec{b}_3 \cdot \delta_3 \qquad \delta_3, \vec{u}_3$$
$$\vec{u}_4 + \vec{b}_4 \cdot \delta_4 \qquad \delta_4, \vec{u}_4$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1 \qquad \delta_1, \vec{u}_1$$

$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2 \qquad \delta_2, \vec{u}_2$$

$$\vec{u}_3 + \vec{b}_3 \cdot \delta_3 \qquad \delta_3, \vec{u}_3$$

$$\vec{u}_4 + \vec{b}_4 \cdot \delta_4 \qquad \delta_4, \vec{u}_4$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\begin{array}{c} \vec{u}_1 + \vec{b}_1 \cdot \delta_1 \\ \vec{u}_2 + \vec{b}_2 \cdot \delta_2 \\ \vec{u}_3 + \vec{b}_3 \cdot \delta_3 \\ \vec{u}_4 + \vec{b}_4 \cdot \delta_4 \end{array} \xrightarrow{\vec{b} - \vec{b}_1} \begin{array}{c} \delta_1, \vec{u}_1 \\ \delta_2, \vec{u}_2 \\ \delta_3, \vec{u}_3 \\ \delta_4, \vec{u}_4 \end{array}$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\begin{array}{lcl}
\vec{u}_1 + \vec{b}_1 \cdot \delta_1 & \xrightarrow{\vec{b} - \vec{b}_1} & \delta_1, \vec{u}_1 - \delta_1 \cdot (\vec{b} - \vec{b}_1) \\
\vec{u}_2 + \vec{b}_2 \cdot \delta_2 & & \delta_2, \vec{u}_2 \\
\vec{u}_3 + \vec{b}_3 \cdot \delta_3 & & \delta_3, \vec{u}_3 \\
\vec{u}_4 + \vec{b}_4 \cdot \delta_4 & & \delta_4, \vec{u}_4
\end{array}$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1 \xrightarrow{\vec{b} - \vec{b}_1} \delta_1, \vec{u}_1 \overbrace{- \delta_1 \cdot (\vec{b} - \vec{b}_1)}^{\vec{u}'_1}$$

$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2 \qquad \delta_2, \vec{u}_2$$

$$\vec{u}_3 + \vec{b}_3 \cdot \delta_3 \qquad \delta_3, \vec{u}_3$$

$$\vec{u}_4 + \vec{b}_4 \cdot \delta_4 \qquad \delta_4, \vec{u}_4$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\vec{u}'_1 + \vec{b} \cdot \delta_1 = \begin{array}{l} \vec{u}_1 + \vec{b}_1 \cdot \delta_1 \\ \vec{u}_2 + \vec{b}_2 \cdot \delta_2 \\ \vec{u}_3 + \vec{b}_3 \cdot \delta_3 \\ \vec{u}_4 + \vec{b}_4 \cdot \delta_4 \end{array} \xrightarrow{\vec{b} - \vec{b}_1} \begin{array}{l} \delta_1, \overbrace{\vec{u}_1 - \delta_1 \cdot (\vec{b} - \vec{b}_1)}^{\vec{u}'_1} \\ \delta_2, \vec{u}_2 \\ \delta_3, \vec{u}_3 \\ \delta_4, \vec{u}_4 \end{array}$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\vec{u}'_1 + \vec{b} \cdot \delta_1 = \vec{u}_1 + \vec{b}_1 \cdot \delta_1 \xrightarrow{\vec{b} - \vec{b}_1} \delta_1, \overbrace{\vec{u}_1 - \delta_1 \cdot (\vec{b} - \vec{b}_1)}^{\vec{u}'_1}$$

$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2 \xrightarrow{\vec{b} - \vec{b}_2} \delta_2, \vec{u}_2$$

$$\vec{u}_3 + \vec{b}_3 \cdot \delta_3 \qquad \delta_3, \vec{u}_3$$

$$\vec{u}_4 + \vec{b}_4 \cdot \delta_4 \qquad \delta_4, \vec{u}_4$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\vec{u}'_1 + \vec{b} \cdot \delta_1 = \begin{array}{l} \vec{u}_1 + \vec{b}_1 \cdot \delta_1 \\ \vec{u}_2 + \vec{b}_2 \cdot \delta_2 \\ \vec{u}_3 + \vec{b}_3 \cdot \delta_3 \\ \vec{u}_4 + \vec{b}_4 \cdot \delta_4 \end{array} \begin{array}{c} \xrightarrow{\vec{b} - \vec{b}_1} \\ \xrightarrow{\vec{b} - \vec{b}_2} \\ \\ \\ \end{array} \begin{array}{l} \delta_1, \overbrace{\vec{u}_1 - \delta_1 \cdot (\vec{b} - \vec{b}_1)}^{\vec{u}'_1} \\ \delta_2, \vec{u}_2 - \delta_2 \cdot (\vec{b} - \vec{b}_2) \\ \delta_3, \vec{u}_3 \\ \delta_4, \vec{u}_4 \end{array}$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n\cdot\delta_2 + n^2\cdot\delta_3 + n^3\cdot\delta_4$$

$$\vec{u}'_1 + \vec{b}\cdot\delta_1 = \begin{array}{lcl} \vec{u}_1 + \vec{b}_1\cdot\delta_1 & \xrightarrow{\vec{b} - \vec{b}_1} & \delta_1, \overbrace{\vec{u}_1 - \delta_1\cdot(\vec{b} - \vec{b}_1)}^{\vec{u}'_1} \\ \vec{u}_2 + \vec{b}_2\cdot\delta_2 & \xrightarrow{\vec{b} - \vec{b}_2} & \delta_2, \vec{u}_2 - \delta_2\cdot(\vec{b} - \vec{b}_2) \\ \vec{u}_3 + \vec{b}_3\cdot\delta_3 & \xrightarrow{\vec{b} - \vec{b}_3} & \delta_3, \vec{u}_3 \\ \vec{u}_4 + \vec{b}_4\cdot\delta_4 & & \delta_4, \vec{u}_4 \end{array}$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\begin{array}{rcl}
\vec{u}_1' + \vec{b} \cdot \delta_1 = \vec{u}_1 + \vec{b}_1 \cdot \delta_1 & \xrightarrow{\vec{b} - \vec{b}_1} & \delta_1,\ \overbrace{\vec{u}_1 - \delta_1 \cdot (\vec{b} - \vec{b}_1)}^{\vec{u}_1'} \\
\vec{u}_2 + \vec{b}_2 \cdot \delta_2 & \xrightarrow{\vec{b} - \vec{b}_2} & \delta_2,\ \vec{u}_2 - \delta_2 \cdot (\vec{b} - \vec{b}_2) \\
\vec{u}_3 + \vec{b}_3 \cdot \delta_3 & \xrightarrow{\vec{b} - \vec{b}_3} & \delta_3,\ \vec{u}_3 - \delta_3 \cdot (\vec{b} - \vec{b}_3) \\
\vec{u}_4 + \vec{b}_4 \cdot \delta_4 & & \delta_4,\ \vec{u}_4
\end{array}$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\vec{u}_1' + \vec{b} \cdot \delta_1 =$$

$$\begin{array}{lcl}
\vec{u}_1 + \vec{b}_1 \cdot \delta_1 & \xrightarrow{\vec{b} - \vec{b}_1} & \delta_1, \underbrace{\vec{u}_1 - \delta_1 \cdot (\vec{b} - \vec{b}_1)}_{\vec{u}_1'} \\
\vec{u}_2 + \vec{b}_2 \cdot \delta_2 & \xrightarrow{\vec{b} - \vec{b}_2} & \delta_2, \vec{u}_2 - \delta_2 \cdot (\vec{b} - \vec{b}_2) \\
\vec{u}_3 + \vec{b}_3 \cdot \delta_3 & \xrightarrow{\vec{b} - \vec{b}_3} & \delta_3, \vec{u}_3 - \delta_3 \cdot (\vec{b} - \vec{b}_3) \\
\vec{u}_4 + \vec{b}_4 \cdot \delta_4 & \xrightarrow{\vec{b} - \vec{b}_4} & \delta_4, \vec{u}_4
\end{array}$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

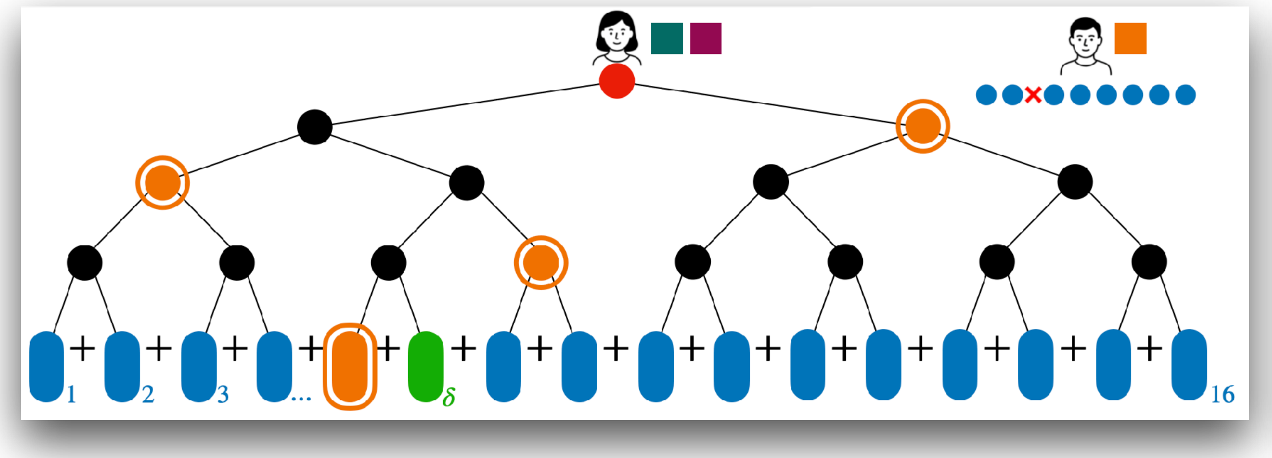
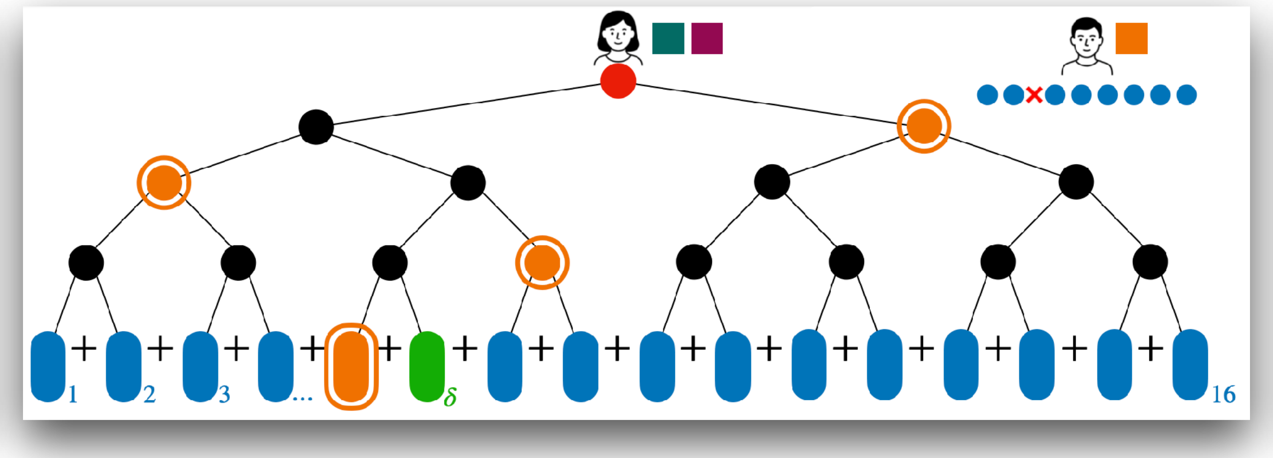
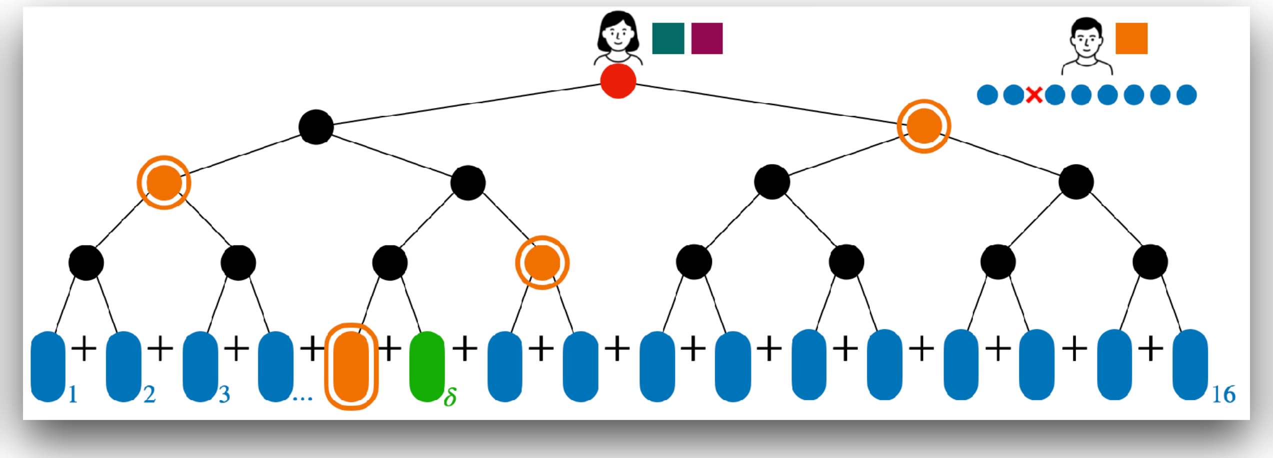
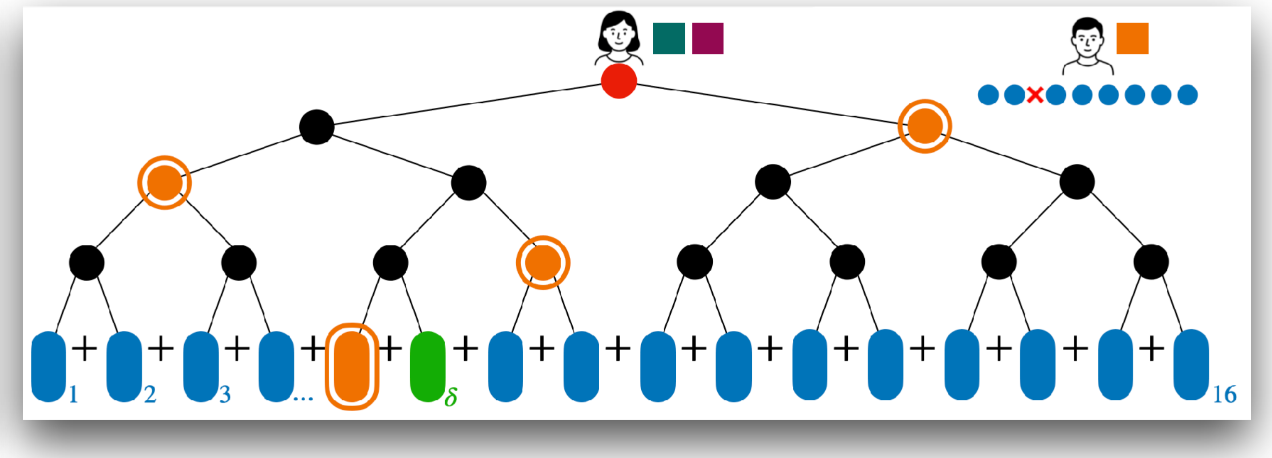
$$\vec{u}'_1 + \vec{b} \cdot \delta_1 = \begin{array}{lcl}
\vec{u}_1 + \vec{b}_1 \cdot \delta_1 & \xrightarrow{\vec{b} - \vec{b}_1} & \delta_1, \underbrace{\vec{u}_1 - \delta_1 \cdot (\vec{b} - \vec{b}_1)}_{\vec{u}'_1} \\
\vec{u}_2 + \vec{b}_2 \cdot \delta_2 & \xrightarrow{\vec{b} - \vec{b}_2} & \delta_2, \vec{u}_2 - \delta_2 \cdot (\vec{b} - \vec{b}_2) \\
\vec{u}_3 + \vec{b}_3 \cdot \delta_3 & \xrightarrow{\vec{b} - \vec{b}_3} & \delta_3, \vec{u}_3 - \delta_3 \cdot (\vec{b} - \vec{b}_3) \\
\vec{u}_4 + \vec{b}_4 \cdot \delta_4 & \xrightarrow{\vec{b} - \vec{b}_4} & \delta_4, \vec{u}_4 - \delta_4 \cdot (\vec{b} - \vec{b}_4)
\end{array}$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n\cdot\delta_2 + n^2\cdot\delta_3 + n^3\cdot\delta_4$$

$$
\begin{array}{rlcl}
 & \vec{u}_1 + \vec{b}_1\cdot\delta_1 & \xrightarrow{\quad \vec{b} - \vec{b}_1 \quad} & \delta_1,\ \vec{u}_1 \overbrace{-\delta_1\cdot(\vec{b} - \vec{b}_1)}^{\vec{u}_1'} \\
+n\times & \vec{u}_2 + \vec{b}_2\cdot\delta_2 & \xrightarrow{\quad \vec{b} - \vec{b}_2 \quad} & \delta_2,\ \vec{u}_2 - \delta_2\cdot(\vec{b} - \vec{b}_2) \\
+n^2\times & \vec{u}_3 + \vec{b}_3\cdot\delta_3 & \xrightarrow{\quad \vec{b} - \vec{b}_3 \quad} & \delta_3,\ \vec{u}_3 - \delta_3\cdot(\vec{b} - \vec{b}_3) \\
+n^3\times & \vec{u}_4 + \vec{b}_4\cdot\delta_4 & \xrightarrow{\quad \vec{b} - \vec{b}_4 \quad} & \delta_4,\ \vec{u}_4 - \delta_4\cdot(\vec{b} - \vec{b}_4)
\end{array}
$$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$\vec{u}'_1$

$\vec{b} - \vec{b}_1$

$\vec{b} - \vec{b}_2$

$+n \times \; \vec{u}_4 + \vec{b}_4 \cdot \delta_4$ $\qquad$ $\delta_4, \; \vec{u}_4 - \delta_4 \cdot (\vec{b} - \vec{b}_4)$

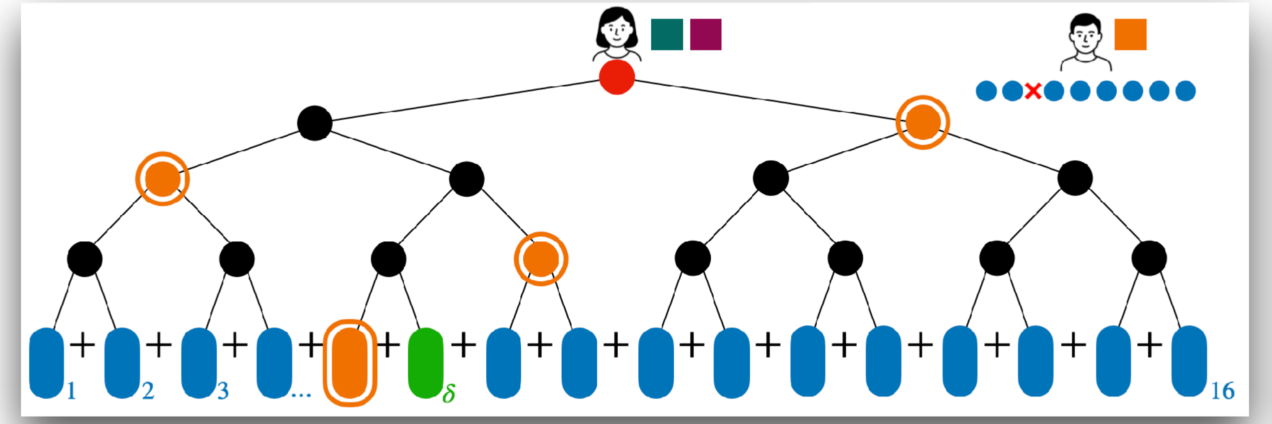
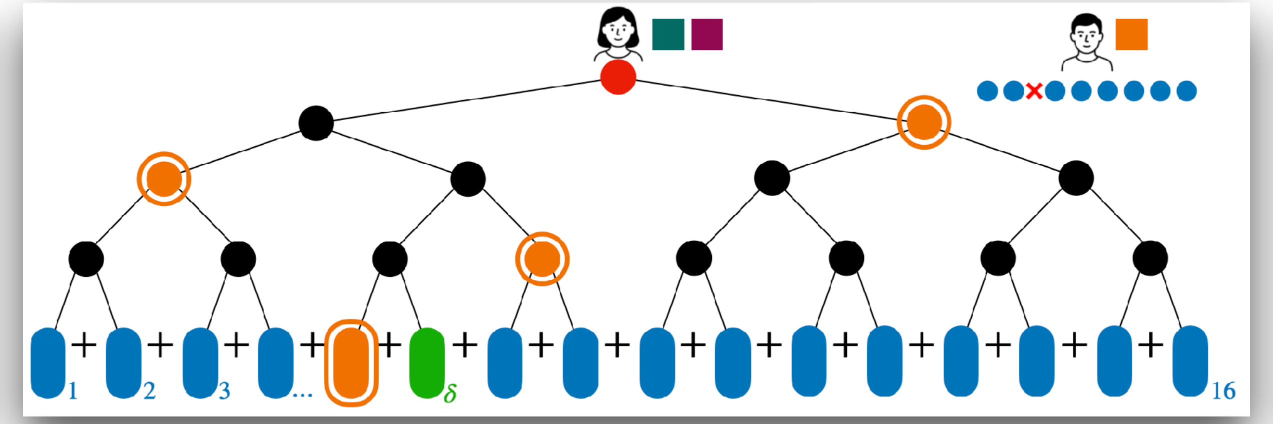
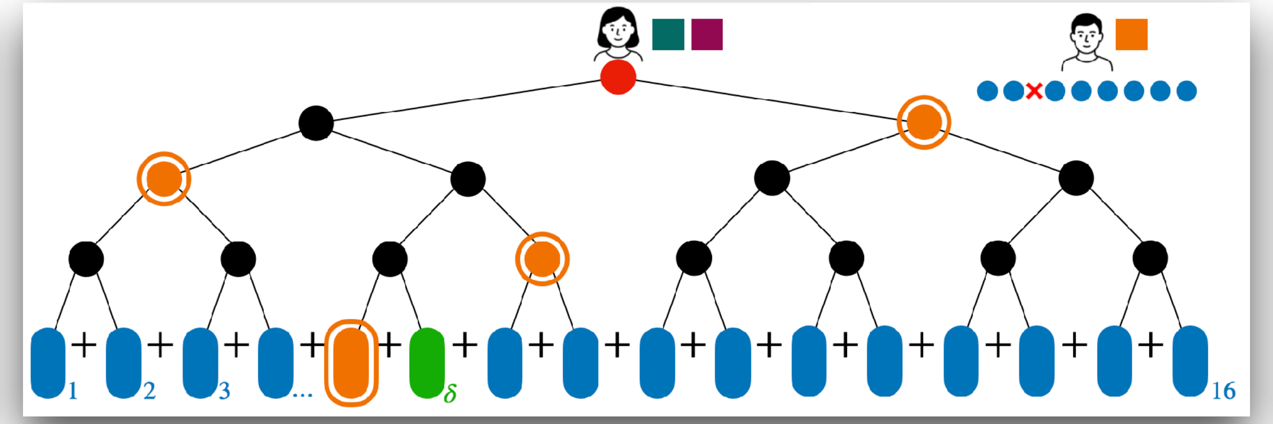
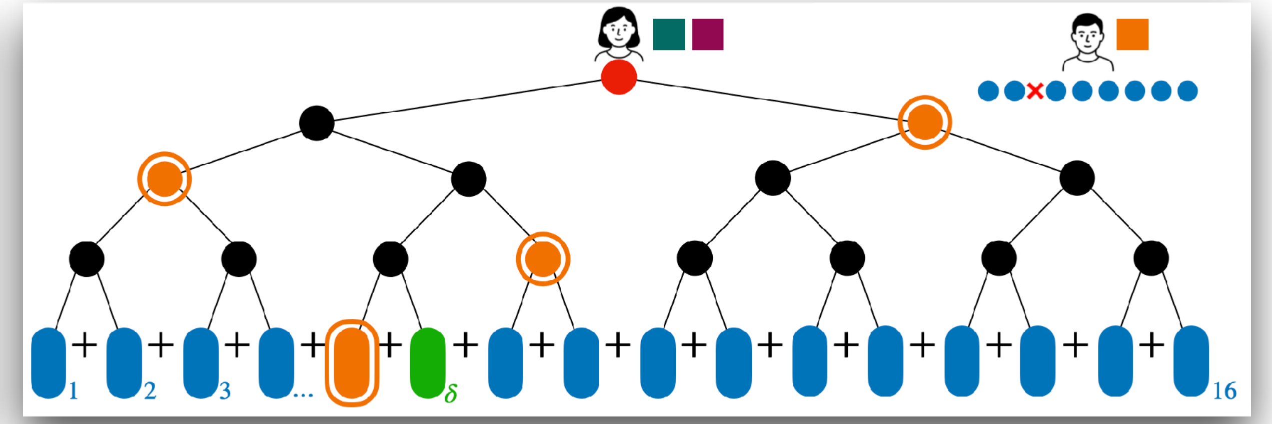
$\vec{b} - \vec{b}_3$

$+n^2 \times$

$\vec{b} - \vec{b}_4$

$+n^3 \times$

Retour aux transferts inconscients corrélés

$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\vec{u} + \vec{b} \cdot \delta$$

$$\delta, \ \vec{u}$$

Retour aux transferts inconscients corrélés

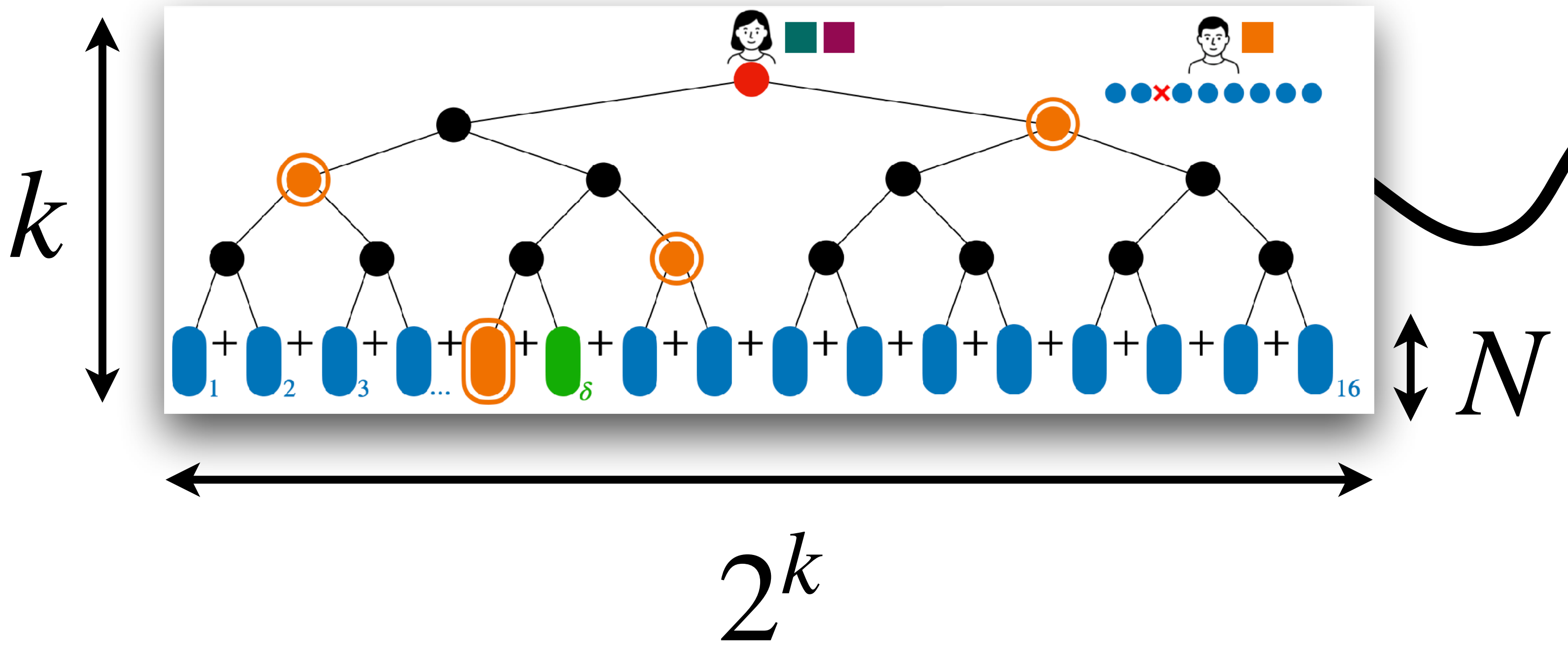
$$\delta = \delta_1 + n \cdot \delta_2 + n^2 \cdot \delta_3 + n^3 \cdot \delta_4$$

$$\vec{u} + \vec{b} \cdot \delta \qquad\qquad \delta,\ \vec{u}$$

$\mathrm{H}(u_1)$	$\mathrm{H}(u_1+\delta)$	$\mathrm{H}(u_1 + b_1 \cdot \delta)$
$\mathrm{H}(u_2)$	$\mathrm{H}(u_2+\delta)$	$\mathrm{H}(u_2 + b_2 \cdot \delta)$
$\mathrm{H}(u_3)$	$\mathrm{H}(u_3+\delta)$	$\mathrm{H}(u_3 + b_3 \cdot \delta)$
$\mathrm{H}(u_4)$	$\mathrm{H}(u_4+\delta)$	$\mathrm{H}(u_4 + b_4 \cdot \delta)$
$\mathrm{H}(u_5)$	$\mathrm{H}(u_5+\delta)$	$\mathrm{H}(u_5 + b_5 \cdot \delta)$
$\mathrm{H}(u_6)$	$\mathrm{H}(u_6+\delta)$	$\mathrm{H}(u_6 + b_6 \cdot \delta)$

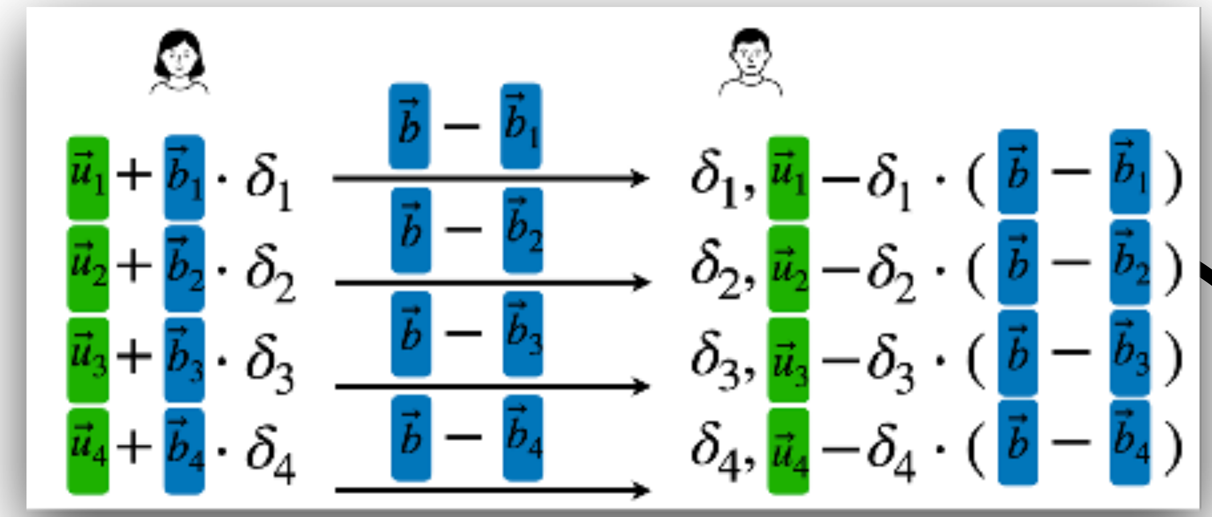
Bilan

Obtenir N transfers inconscients, combien ça coûte ?



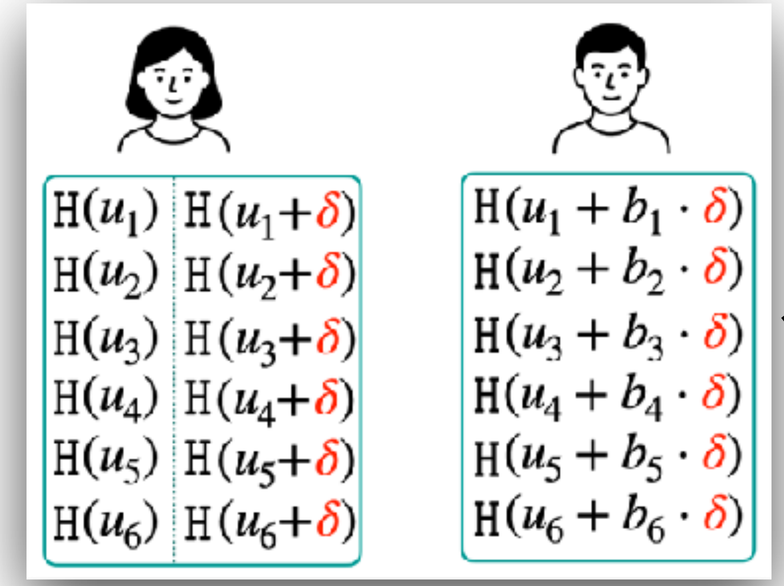
- 2^k appels à un PRG (pour l'arbre)
- $2^k N/128$ appels à un PRG (pour les feuilles)
- k invocations d'un transfert inconscient (noeuds oranges)

Une exécution donne un δ avec k bits d'entropie $\Longrightarrow$ on répète $128/k \times$ pour avoir 128 bits



- $128 \times 2^k/k$ appels à un PRG (pour l'arbre)
- $2^k N/k$ appels à un PRG (pour les feuilles)
- 128 invocations d'un transfert inconscient (noeuds oranges)
- $128 \times N/k$ bits de communication (« dérandomiser $\vec{b}$ »)

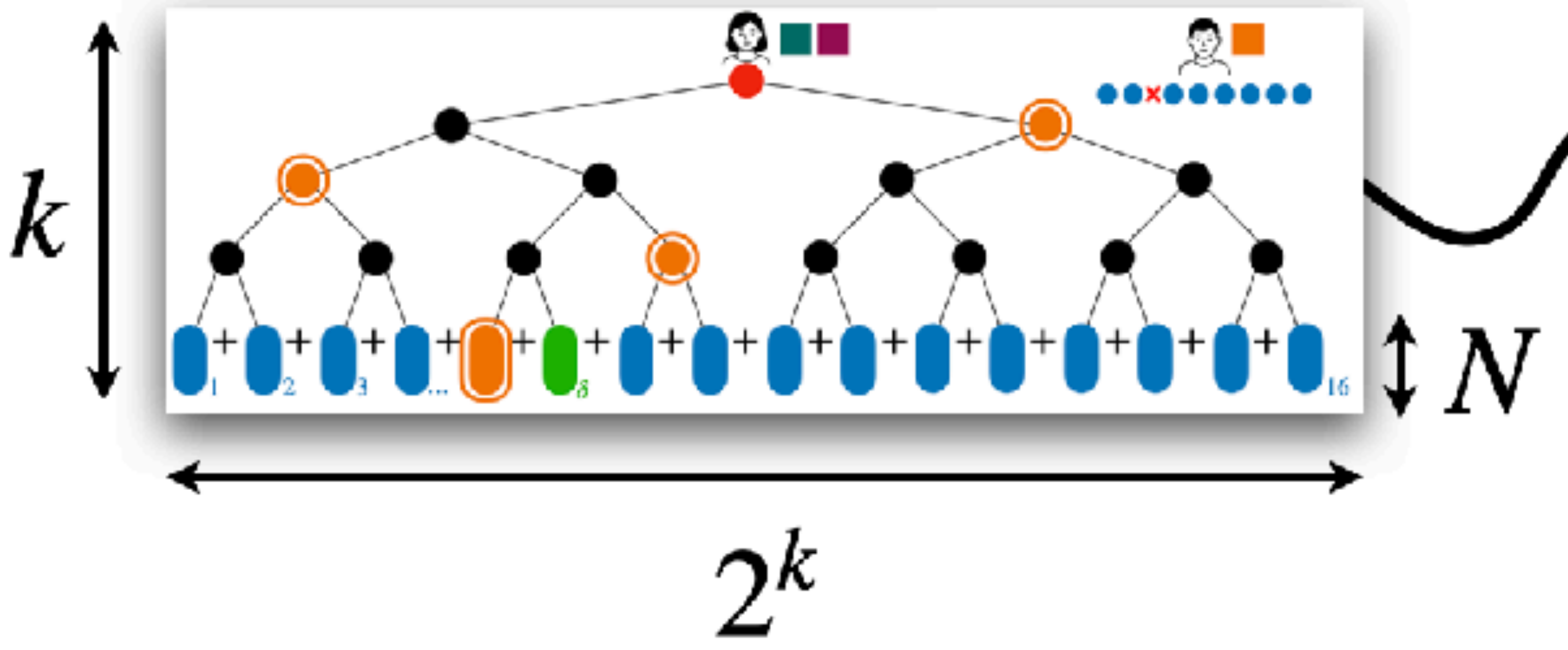
Enfin, on converti tout ça en TI avec une fonction de hachage :



- $2N$ appels à une fonction de hachage

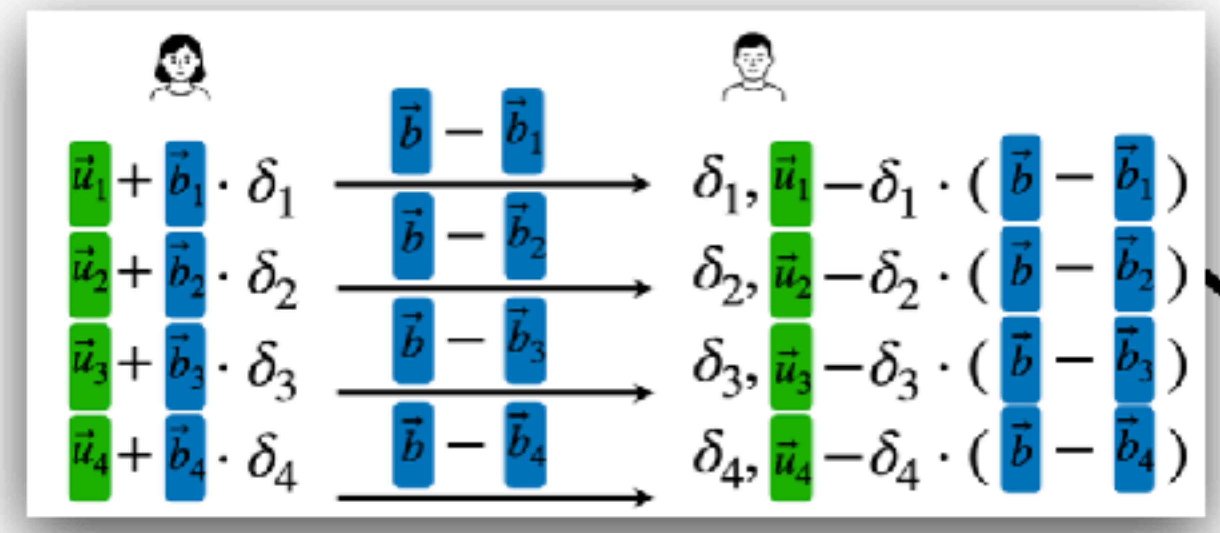
Bilan

Obtenir N transferts inconscients, combien ça coûte ?



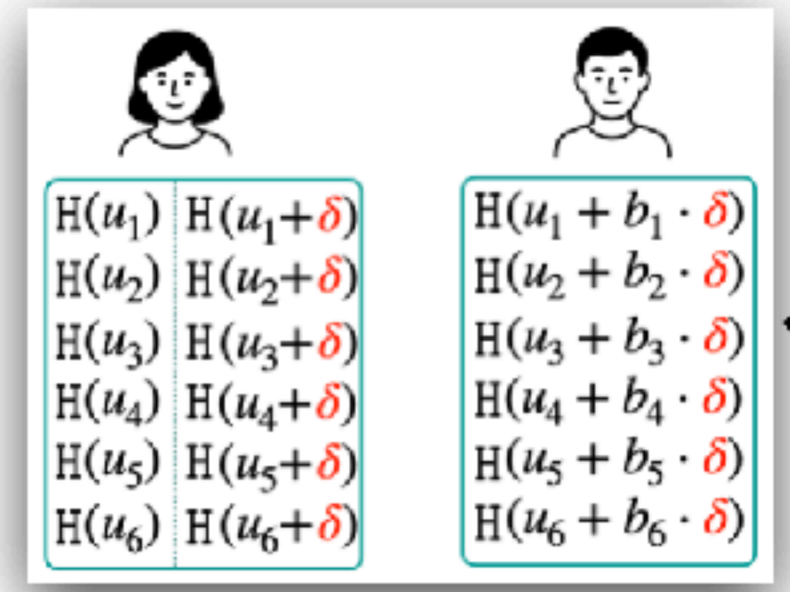
- 2^k appels à un PRG (pour l'arbre)
- $2^k N/128$ appels à un PRG (pour les feuilles)
- k invocations d'un transfert inconscient (noeuds oranges)

Une exécution donne un δ avec k bits d'entropie $\Longrightarrow$ on répète $128/k\,\times$ pour avoir 128 bits



- $128 \times 2^k/k$ appels à un PRG (pour l'arbre)
- $2^k N/k$ appels à un PRG (pour les feuilles)
- 128 invocations d'un transfert inconscient (noeuds oranges)
- $128 \times N/k$ bits de communication (« dérandomiser $\vec{b}$ »)

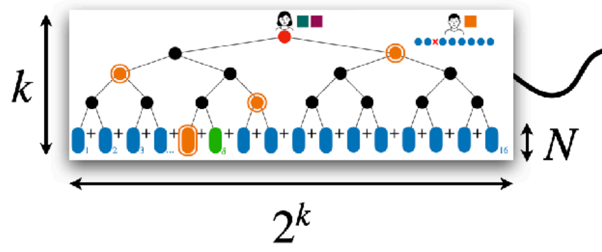
Enfin, on converti tout ça en TI avec une fonction de hachage :



- $2N$ appels à une fonction de hachage

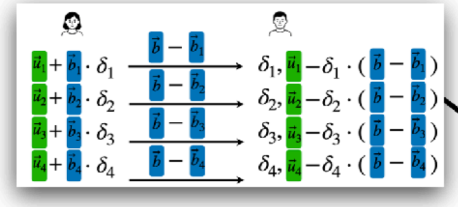
Bilan

Obtenir N transfers inconscients, combien ça coûte ?



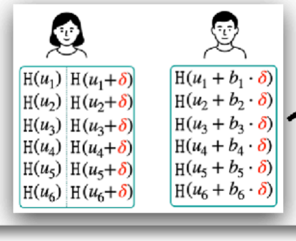
- 2^k appels à un PRG (pour l'arbre)
- $2^k N/128$ appels à un PRG (pour les feuilles)
- k invocations d'un transfert inconscient (noeuds oranges)

Une exécution donne un δ avec k bits d'entropie $\Longrightarrow$ on répète $128/k\times$ pour avoir 128 bits



- $128 \times 2^k/k$ appels à un PRG (pour l'arbre)
- $2^k N/k$ appels à un PRG (pour les feuilles)
- 128 invocations d'un transfert inconscient (noeuds oranges)
- $128 \times N/k$ bits de communication (« dérandomiser $\vec{b}$ »)

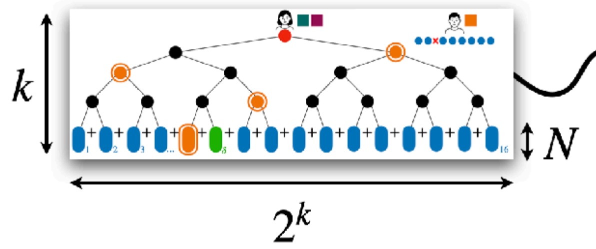
Enfin, on converti tout ça en TI avec une fonction de hachage :



- $2N$ appels à une fonction de hachage

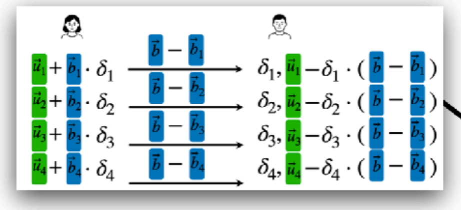
Bilan

Obtenir N transfers inconscients, combien ça coûte ?



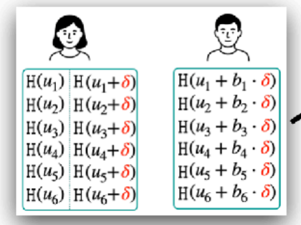
- 2^k appels à un PRG (pour l'arbre)
- $2^kN/128$ appels à un PRG (pour les feuilles)
- k invocations d'un transfert inconscient (noeuds oranges)

Une exécution donne un δ avec k bits d'entropie $\Longrightarrow$ on répète $128/k \times$ pour avoir 128 bits



- $128 \times 2^k/k$ appels à un PRG (pour l'arbre)
- $2^kN/k$ appels à un PRG (pour les feuilles)
- 128 invocations d'un transfert inconscient (noeuds oranges)
- $128 \times N/k$ bits de communication (« dérandomiser $\vec{b}$ »)

Enfin, on converti tout ça en TI avec une fonction de hachage :



- $2N$ appels à une fonction de hachage

$k = 2$:

: 53 millions OT/s (× 13250)

: 8 octets (÷ 16)

: 1200 heures → 5.9 minutes **/ #coeurs**

: 1.1 To → 69 Go

$k = 8$:

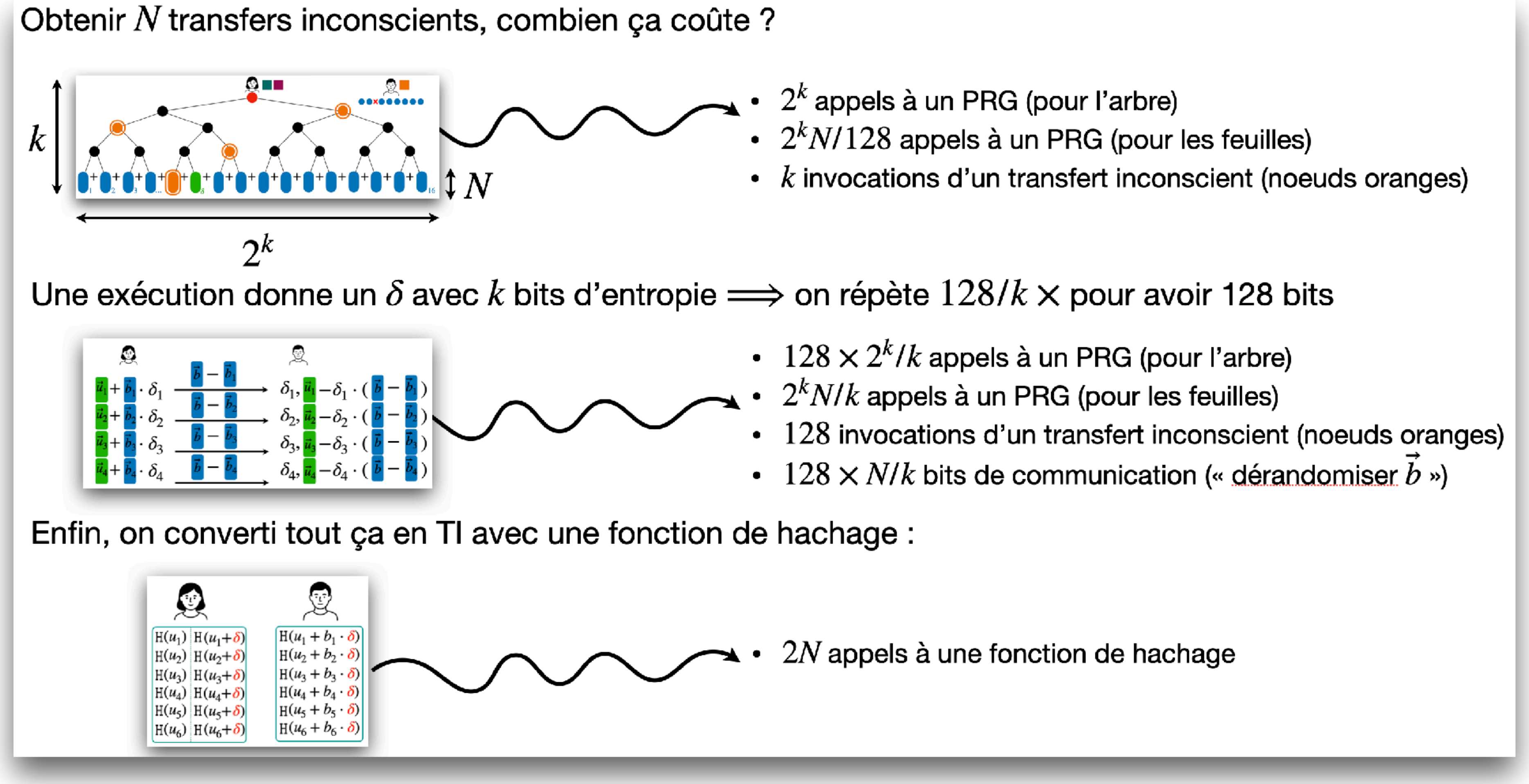
: 9.5 millions OT/s (× 2375)

: 2 octets (÷ 64)

: 1200 heures → 33 minutes **/ #coeurs**

: 1.1 To → 17 Go

Bilan



Obtenir N transferts inconscients, combien ça coûte ?

- 2^k appels à un PRG (pour l'arbre)
- $2^k N/128$ appels à un PRG (pour les feuilles)
- k invocations d'un transfert inconscient (noeuds oranges)

Une exécution donne un δ avec k bits d'entropie $\Longrightarrow$ on répète $128/k \times$ pour avoir 128 bits

- $128 \times 2^k/k$ appels à un PRG (pour l'arbre)
- $2^k N/k$ appels à un PRG (pour les feuilles)
- 128 invocations d'un transfert inconscient (noeuds oranges)
- $128 \times N/k$ bits de communication (« dérandomiser $\vec{b}$ »)

Enfin, on converti tout ça en TI avec une fonction de hachage :

- $2N$ appels à une fonction de hachage

Augmenter le nombre de coeurs est « facile »

Augmenter la bande passante est plus difficile !

?

Comment réduire la bande passante ?

$k = 2$:

: 53 millions OT/s (× 13250)

: 8 octets (÷ 16)

: 1200 heures → 5.9 minutes **/ #coeurs**

: 1.1 To → 69 Go

$k = 8$:

: 9.5 millions OT/s (× 2375)

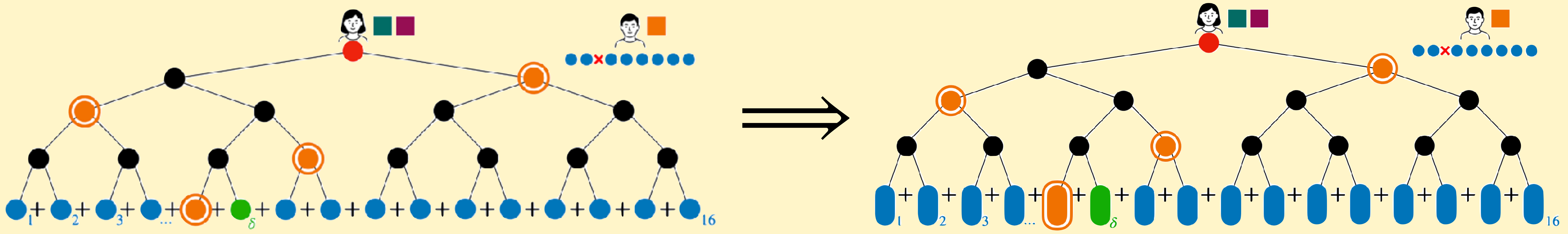
: 2 octets (÷ 64)

: 1200 heures → 33 minutes **/ #coeurs**

: 1.1 To → 17 Go

Ouverture I : réduire la bande-passante

1



2

$$\boxed{\sum_{i=1}^{16} i \cdot \bullet_i} + \boxed{\sum_{i=1}^{16} (\delta - i) \cdot \bullet_i} = \delta \cdot \sum_{i=1}^{16} \bullet_i = \vec{b} \cdot \delta$$

3

$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1 \xrightarrow{\vec{b} - \vec{b}_1} \delta_1, \vec{u}_1 - \delta_1 \cdot (\vec{b} - \vec{b}_1)$$

$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2 \xrightarrow{\vec{b} - \vec{b}_2} \delta_2, \vec{u}_2 - \delta_2 \cdot (\vec{b} - \vec{b}_2)$$

$$\vec{u}_3 + \vec{b}_3 \cdot \delta_3 \xrightarrow{\vec{b} - \vec{b}_3} \delta_3, \vec{u}_3 - \delta_3 \cdot (\vec{b} - \vec{b}_3)$$

$$\vec{u}_4 + \vec{b}_4 \cdot \delta_4 \xrightarrow{\vec{b} - \vec{b}_4} \delta_4, \vec{u}_4 - \delta_4 \cdot (\vec{b} - \vec{b}_4)$$

Ouverture I : réduire la bande-passante

2

$$\boxed{\sum_{i=1}^{16} i \cdot \bullet_i} + \boxed{\sum_{i=1}^{16} (\delta - i) \cdot \bullet_i} = \delta \cdot \sum_{i=1}^{16} \bullet_i = \vec{b} \cdot \delta$$

3

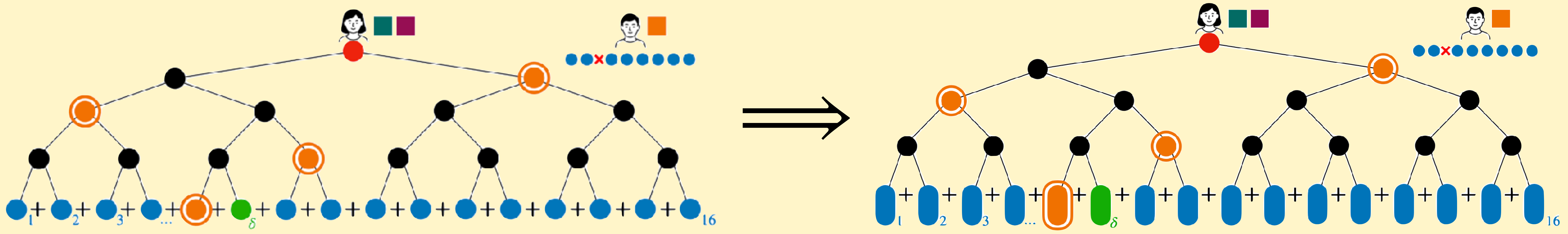
$$\vec{u}_1 + \vec{b}_1 \cdot \delta_1 \xrightarrow{\vec{b} - \vec{b}_1} \delta_1, \vec{u}_1 - \delta_1 \cdot (\vec{b} - \vec{b}_1)$$

$$\vec{u}_2 + \vec{b}_2 \cdot \delta_2 \xrightarrow{\vec{b} - \vec{b}_2} \delta_2, \vec{u}_2 - \delta_2 \cdot (\vec{b} - \vec{b}_2)$$

$$\vec{u}_3 + \vec{b}_3 \cdot \delta_3 \xrightarrow{\vec{b} - \vec{b}_3} \delta_3, \vec{u}_3 - \delta_3 \cdot (\vec{b} - \vec{b}_3)$$

$$\vec{u}_4 + \vec{b}_4 \cdot \delta_4 \xrightarrow{\vec{b} - \vec{b}_4} \delta_4, \vec{u}_4 - \delta_4 \cdot (\vec{b} - \vec{b}_4)$$

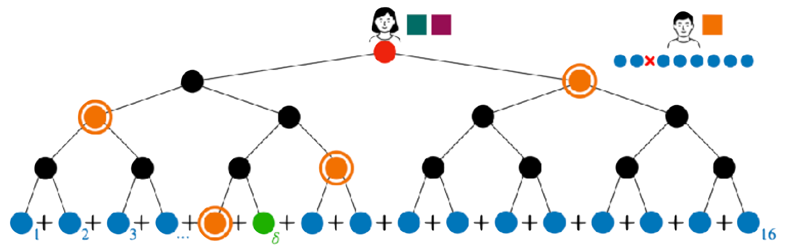
1



Ouverture I : réduire la bande-passante

On utilise un PRG linéairement homomorphe

$$\mathrm{PRG}(\alpha) \qquad \mathrm{PRG}(\beta)$$

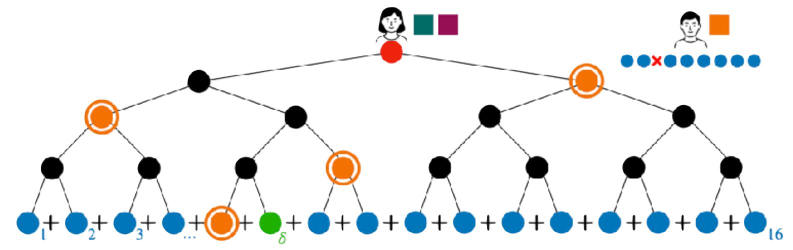


$$\mathrm{PRG}(\alpha + \beta \cdot \delta) \rightarrow \vec{u} + \vec{b} \cdot \delta$$

Ouverture I : réduire la bande-passante

On utilise un PRG linéairement homomorphe

$$\mathrm{PRG}(\alpha) \quad \mathrm{PRG}(\beta)$$



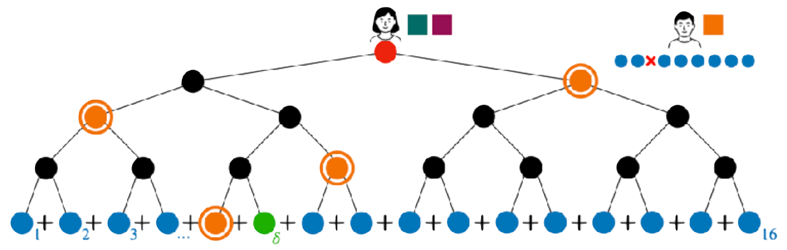
$$\mathrm{PRG}(\alpha + \beta \cdot \delta) \rightarrow \vec{u} + \vec{b} \cdot \delta$$

Quel PRG pourrait convenir ?

Ouverture I : réduire la bande-passante

On utilise un PRG linéairement homomorphe

$$\mathrm{PRG}(\alpha) \quad \mathrm{PRG}(\beta)$$



$$\mathrm{PRG}(\alpha + \beta \cdot \delta) \to \vec{u} + \vec{b} \cdot \delta$$

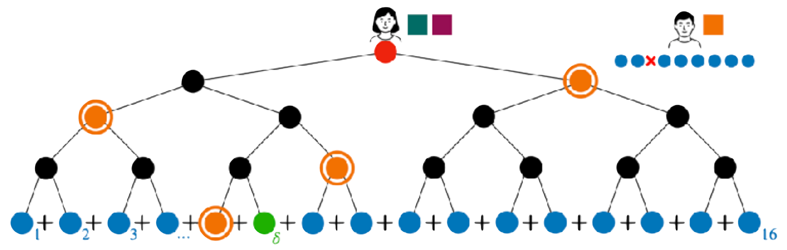
Quel PRG pourrait convenir ?

$$\mathrm{PRG}(\;) \to M \cdot$$

Ouverture I : réduire la bande-passante

On utilise un PRG linéairement homomorphe

$$\mathrm{PRG}(\alpha) \quad \mathrm{PRG}(\beta)$$



$$\mathrm{PRG}(\alpha + \beta \cdot \delta) \rightarrow \vec{u} + \vec{b} \cdot \delta$$

Quel PRG pourrait convenir ?

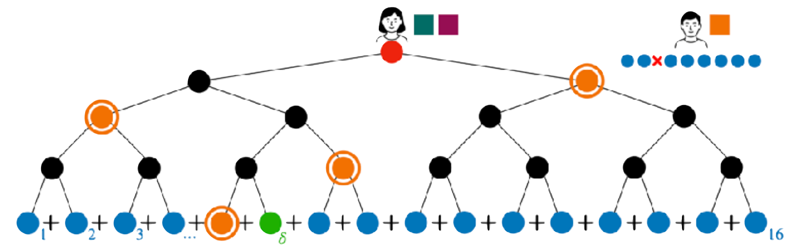
$$\mathrm{PRG}(\;) \rightarrow M \cdot$$

Évidemment, c'est cassé…
Donc on rajoute du bruit !

Ouverture I : réduire la bande-passante

On utilise un PRG linéairement homomorphe

$$\mathrm{PRG}(\alpha) \quad \mathrm{PRG}(\beta)$$



$$\mathrm{PRG}(\alpha + \beta \cdot \delta) \to \vec{u} + \vec{b} \cdot \delta$$

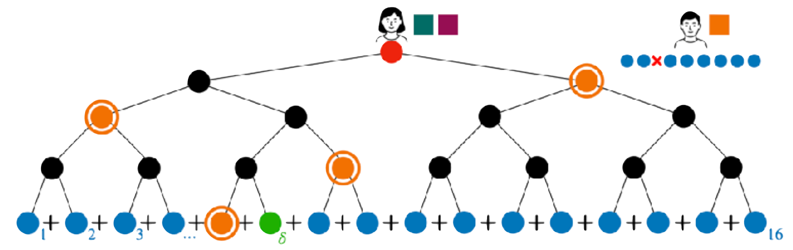
Quel PRG pourrait convenir ?

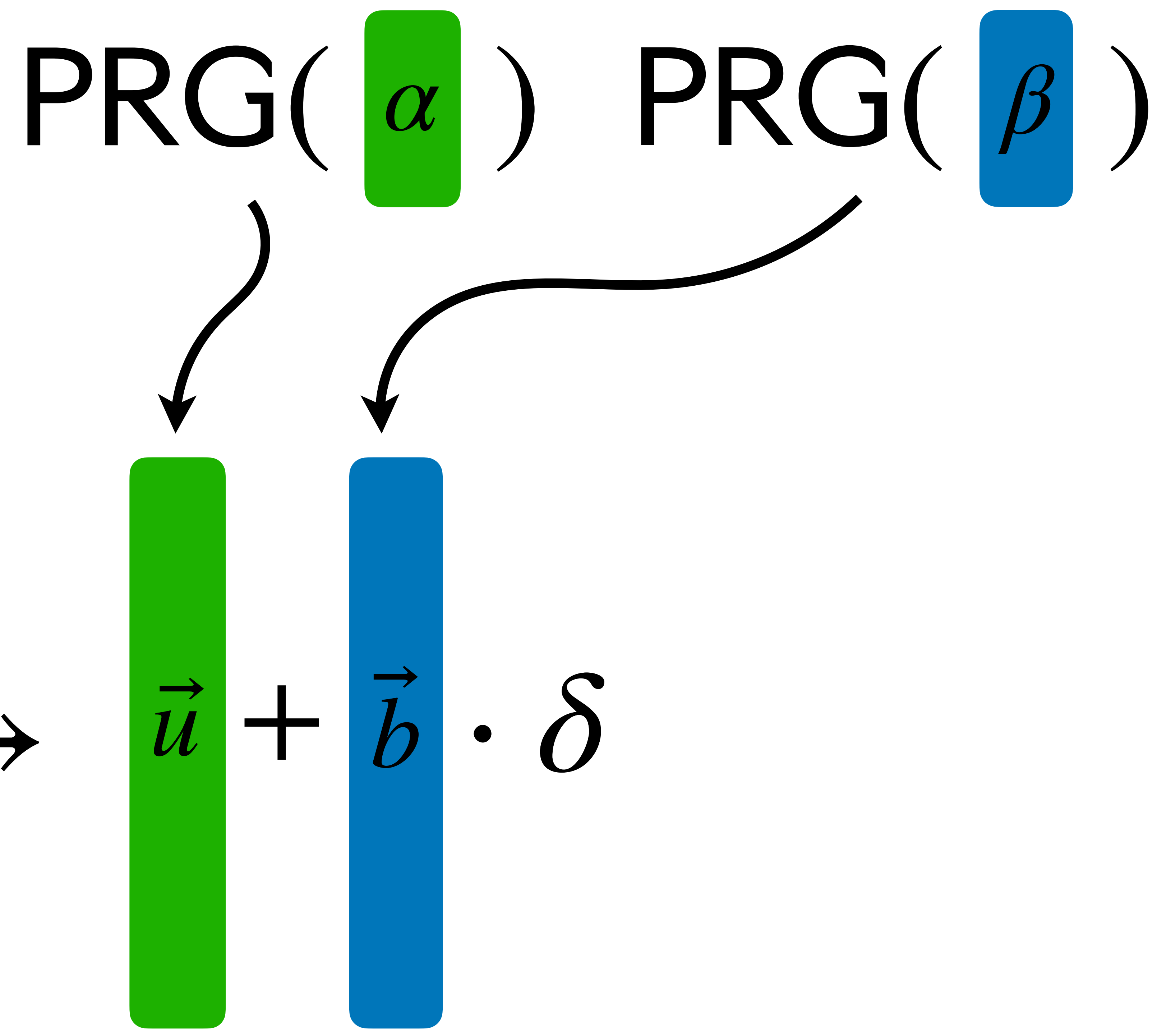
$$\mathrm{PRG}(\square) \to M \cdot \square + e$$

Évidemment, c'est cassé…
Donc on rajoute du bruit !

Ouverture I : réduire la bande-passante

On utilise un PRG linéairement homomorphe

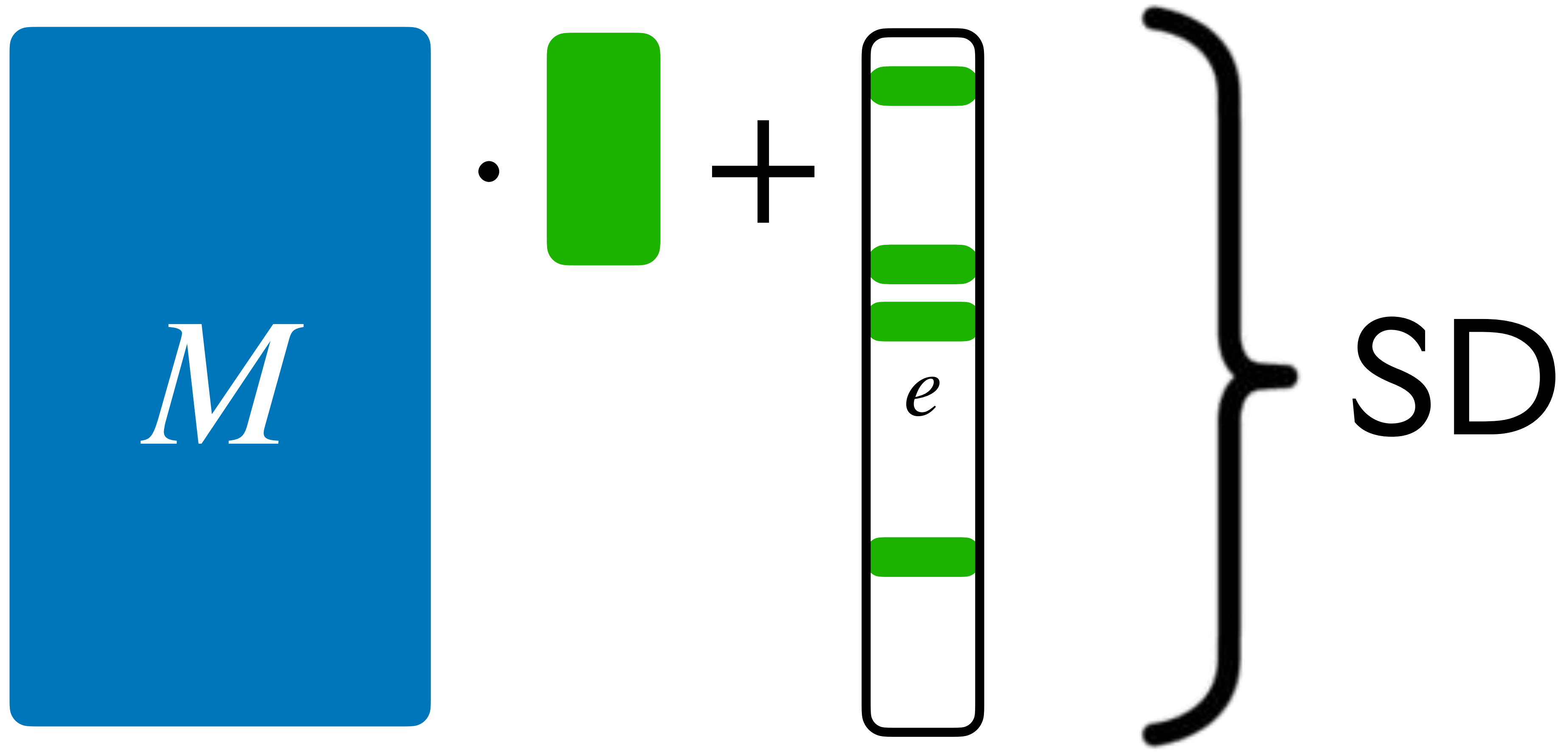




$$\mathrm{PRG}(\alpha + \beta \cdot \delta) \to \vec{u} + \vec{b} \cdot \delta$$

Quel PRG pourrait convenir ?

$$\mathrm{PRG}(\;) \to$$

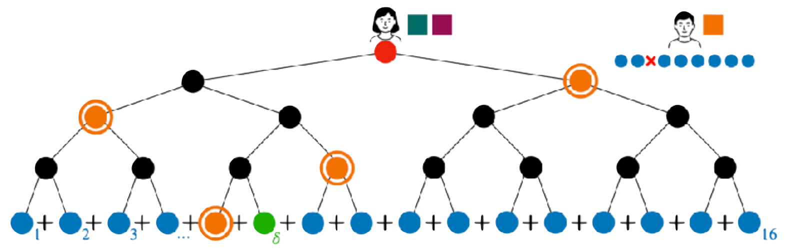


Évidemment, c'est cassé…
Donc on rajoute du bruit !

Ouverture I : réduire la bande-passante

On utilise un PRG linéairement homomorphe

$$\mathrm{PRG}(\alpha) \quad \mathrm{PRG}(\beta)$$



$$\mathrm{PRG}(\alpha + \beta \cdot \delta) \rightarrow \vec{u} + \vec{b} \cdot \delta +$$

Quel PRG pourrait convenir ?

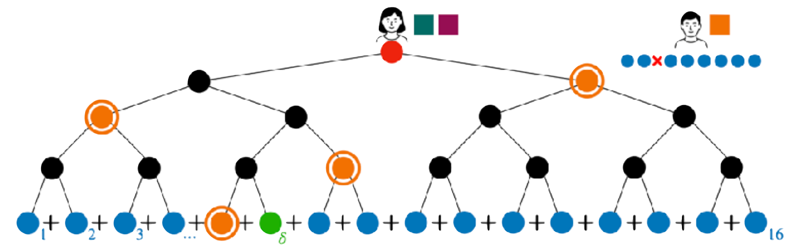
$$\left.\mathrm{PRG}(\ ) \rightarrow M \cdot \ + e\ \right\} \text{SD}$$

Évidemment, c'est cassé…
Donc on rajoute du bruit !

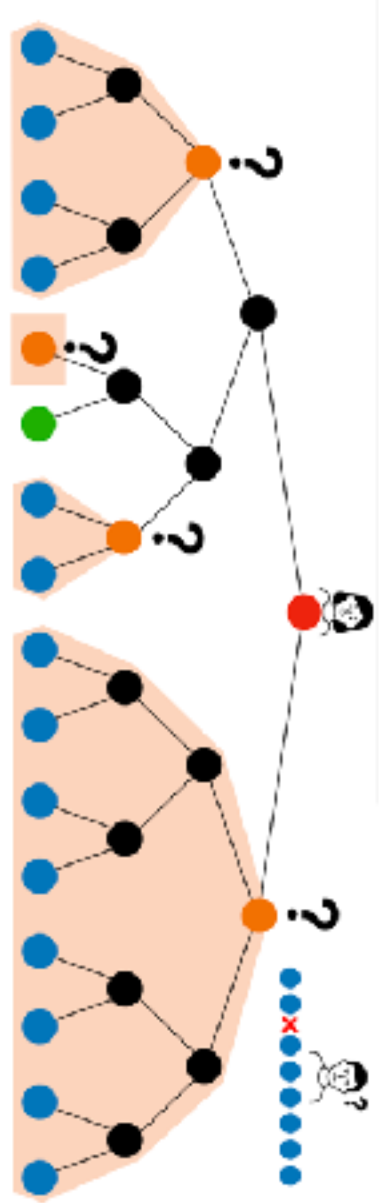
Ouverture I : réduire la bande-passante

On utilise un PRG linéairement homomorphe

$\mathrm{PRG}(\alpha) \quad \mathrm{PRG}(\beta)$



$$\mathrm{PRG}(\alpha + \beta \cdot \delta) \rightarrow \vec{u} + \vec{b} \cdot \delta +$$



Quel PRG pourrait convenir ?

$$\left.\begin{array}{l}\mathrm{PRG}(\;) \rightarrow M \cdot \;\; + e\end{array}\right\} \mathrm{SD}$$

Évidemment, c'est cassé…
Donc on rajoute du bruit !

Bilan

Avec des PCGs :

/ #coeurs

Bilan

Avec des PCGs :

 : 7 millions OT/s ($\times$ 1750)

 : 0 octets ($\div$ ∞)

 : 1200 heures → 45 minutes **/ #coeurs**

 : 1.1 To → 10 Ko

Ouverture II : autres corrélations

Aléa corrélé	Modèle		
ROT	GMW (Circuits Booléens, 2 joueurs, semi-honnête)	(r_0, r_1)	(σ, r_σ)
ROLE($\mathbb{F}$)	Circuits arithmétiques, 2 joueurs, semi-honnête	(u, v)	$(x, ux + v)$
Triplets authentifiés	Circuits arithmétiques, 2 joueurs, malicieux	Parts additives $\langle a, b, ab, \Delta a, \Delta b, \Delta ab \rangle$ pour un MAC Δ	
Triplets matriciels	Algèbre linéaire, 2 joueurs, semi-honnête	Parts additives $\langle A, B, A \cdot B \rangle$	
Autres : corrélations de haut degré, tables de vérité à usage unique, parts de vecteurs unitaires…	Divers protocoles spécialisés : requêtes à une BDD, statistiques…	(Divers)	

Ouverture II : autres corrélations

Aléa corrélé	Modèle		
ROT	GMW (Circuits Booléens, 2 joueurs, semi-honnête)	(r_0, r_1)	(σ, r_σ)
ROLE($\mathbb{F}$)	Circuits arithmétiques, 2 joueurs, semi-honnête	(u, v)	$(x, ux + v)$
Triplets authentifiés	Circuits arithmétiques, 2 joueurs, malicieux	Parts additives $\langle a, b, ab, \Delta a, \Delta b, \Delta ab \rangle$ pour un MAC Δ	
Triplets matriciels	Algèbre linéaire, 2 joueurs, semi-honnête	Parts additives $\langle A, B, A \cdot B \rangle$	
Autres : corrélations de haut degré, tables de vérité à usage unique, parts de vecteurs unitaires…	Divers protocoles spécialisés : requêtes à une BDD, statistiques…	(Divers)	

Ouverture II : autres corrélations

Aléa corrélé	Modèle		
ROT	GMW (Circuits Booléens, 2 joueurs, semi-honnête)	(r_0, r_1)	(σ, r_σ)
ROLE($\mathbb{F}$)	Circuits arithmétiques, 2 joueurs, semi-honnête	(u, v)	$(x, ux + v)$
Triplets authentifiés	Circuits arithmétiques, 2 joueurs, malicieux	Parts additives $\langle a, b, ab, \Delta a, \Delta b, \Delta ab \rangle$ pour un MAC Δ	
Triplets matriciels	Algèbre linéaire, 2 joueurs, semi-honnête	Parts additives $\langle A, B, A \cdot B \rangle$	
Autres : corrélations de haut degré, tables de vérité à usage unique, parts de vecteurs unitaires…	Divers protocoles spécialisés : requêtes à une BDD, statistiques…	(Divers)	

- Gilboa'99 : à partir de $\log |\mathbb{F}|$ OTs
- PCGs pour ROLE (Crypto'20, Crypto'22) : à partir de codes quasi-abéliens

Merci pour votre attention !

Pour aller plus loin :

- *A pragmatic introduction to secure computation*, D. Evans, V. Kolesnikov, M. Rosulek
- Getting started on pseudorandom correlation generators
  (Blogpost, geoffroycouteau.github.io/posts/pcg/)
- *An introduction to silent secure computation*, G. Couteau