Calculer ensemble, sans rien révéler

Guilhem Castagnos

Université de Bordeaux

Bordeaux
12 mars 2021

université de BORDEAUX

Problématique

- Alice et Bob sont à leur premier rendez vous
- Ils veulent savoir s'ils auront un second rendez vous

Mais...

Problématique

- Alice et Bob sont à leur premier rendez vous
- Ils veulent savoir s'ils auront un second rendez vous

Mais...

Ils sont un peu timides !

- Éviter la situation embarrassante :
  l'un d'eux ne veut pas continuer, mais sait que l'autre aurait aimé le faire

Problématique

- Alice et Bob sont à leur premier rendez vous
- Ils veulent savoir s'ils auront un second rendez vous

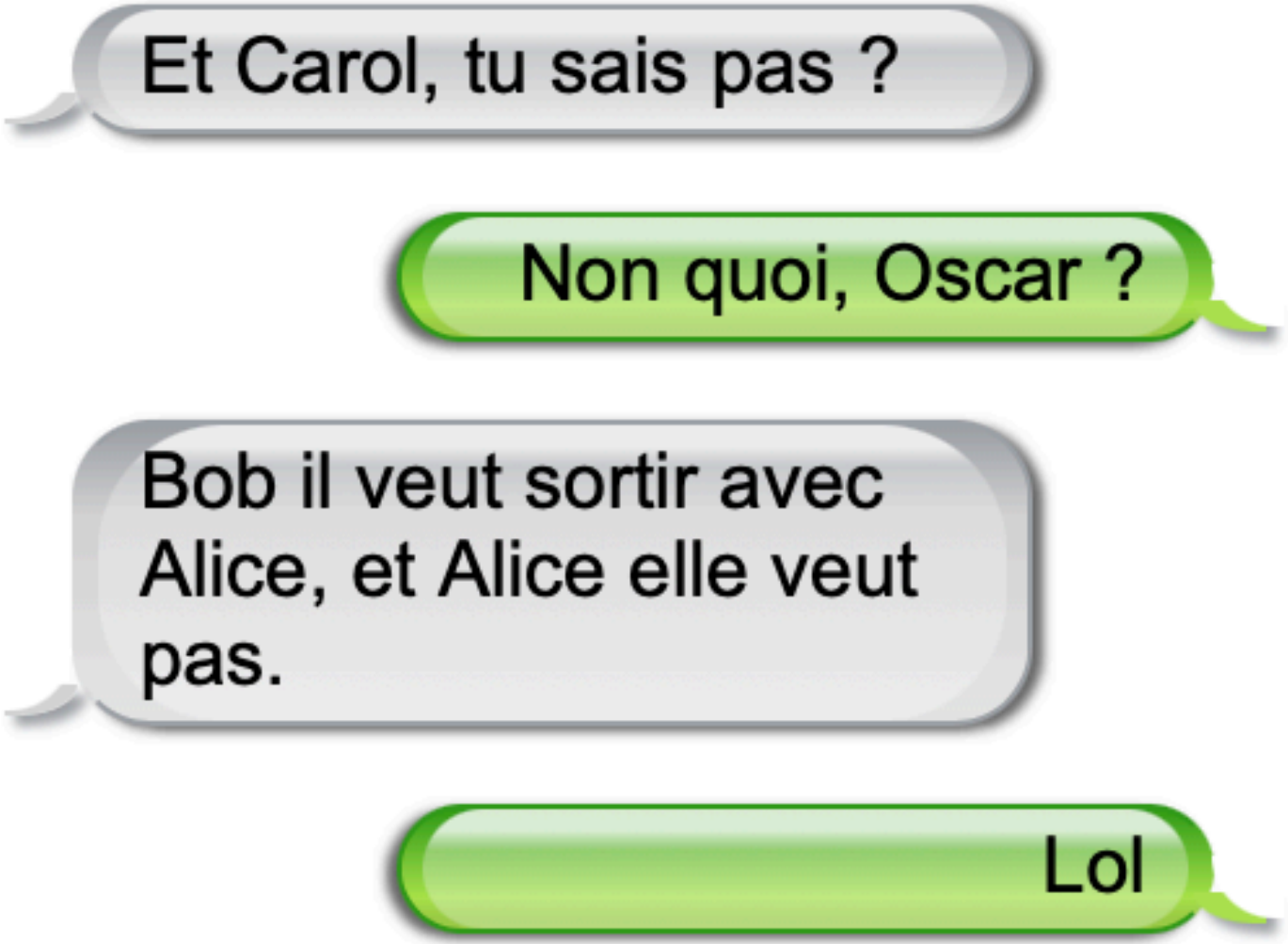
Mais...

Ils sont un peu timides !

- Éviter la situation embarrassante :
  l'un d'eux ne veut pas continuer, mais sait que l'autre aurait aimé le faire

- Une **solution** : passer par Oscar en qui on peut avoir confiance

Problématique

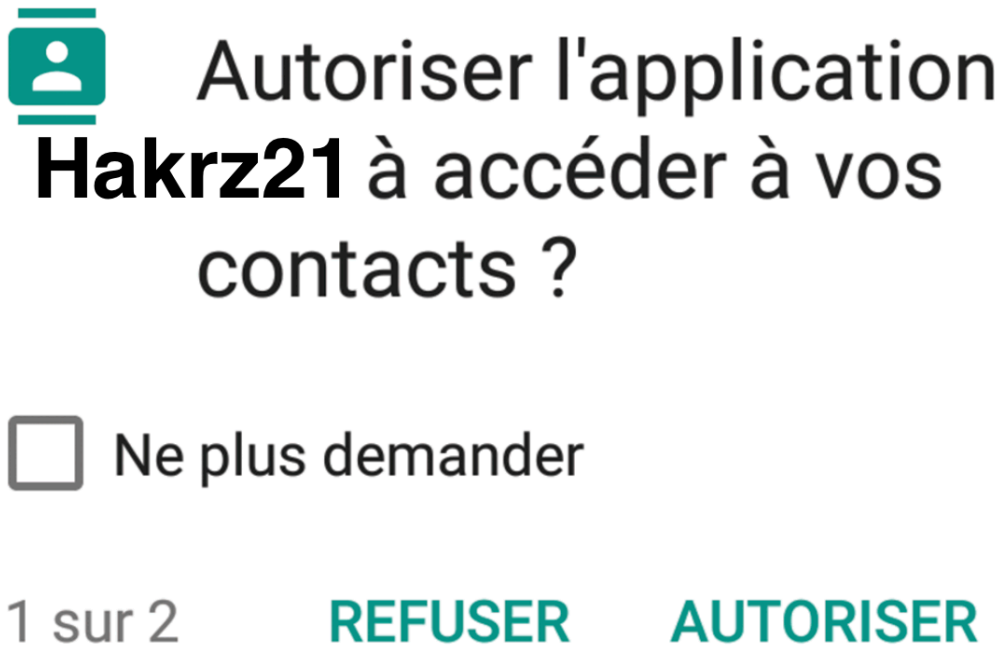


Autre problématique

- Oscar invite Alice sur le nouveau réseau social Hakrz21
- Alice installe l'application sur son téléphone
  Mais...

Autre problématique

- Oscar invite Alice sur le nouveau réseau social Hakrz21
- Alice installe l'application sur son téléphone
  Mais...



Une dernière problématique

- Alice et ses collègues veulent calculer la moyenne de leurs salaires
- **Solutions** :

Une dernière problématique

- Alice et ses collègues veulent calculer la moyenne de leurs salaires
- **Solutions** :
  - Révéler son salaire à tous...

Une dernière problématique

- Alice et ses collègues veulent calculer la moyenne de leurs salaires
- **Solutions** :
  - Révéler son salaire à tous...
  - Passer par Oscar en qui...

LA solution

Utiliser la cryptographie :

LA solution

Utiliser la cryptographie :

Le **calcul multipartite sécurisé**

Calcul multipartite sécurisé

- Plusieurs parties : $P_1, P_2 \dots, P_n$
- Chaque partie à un secret s_i
- Les parties veulent calculer ensemble sans tiers de confiance

$$f(s_1, s_2, \dots, s_n)$$

- Toutes les parties apprennent le résultat mais rien d'autre

Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$
- On veut calculer

$$f(s_1, s_2, \dots, s_n) = \sum_{i=1}^{n} s_i/n$$

Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$
- On veut calculer

$$f(s_1, s_2, \dots, s_n) = \sum_{i=1}^{n} s_i$$

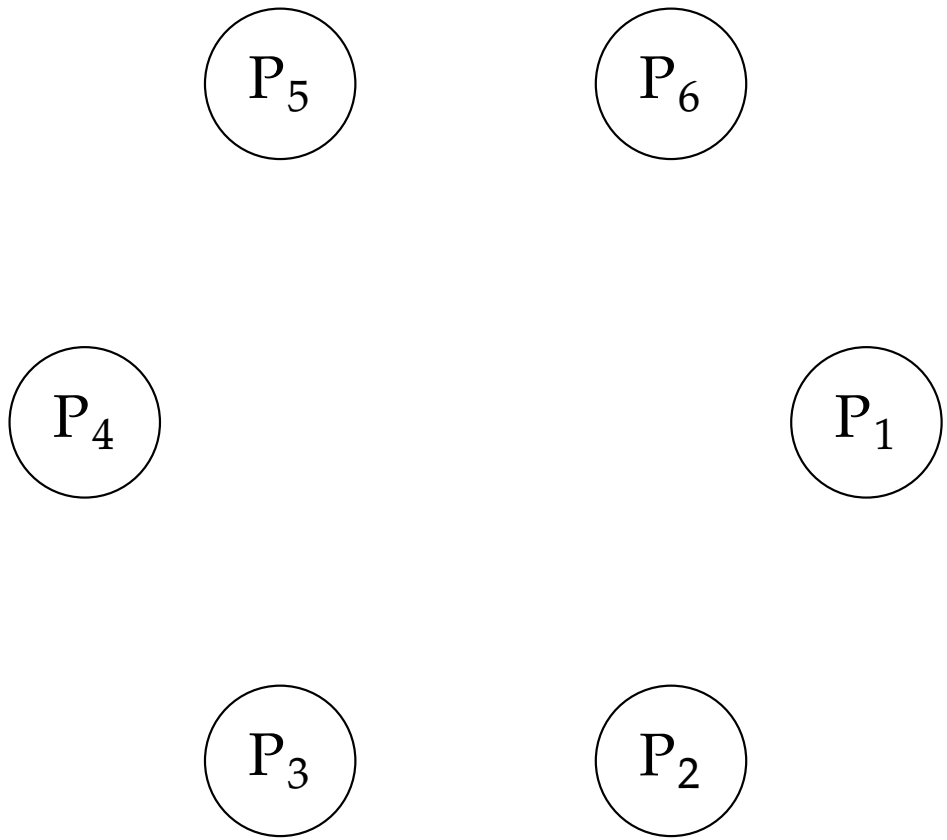
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$
- On veut calculer

$$f(s_1, s_2, \ldots, s_n) = \sum_{i=1}^{n} s_i \mod M$$

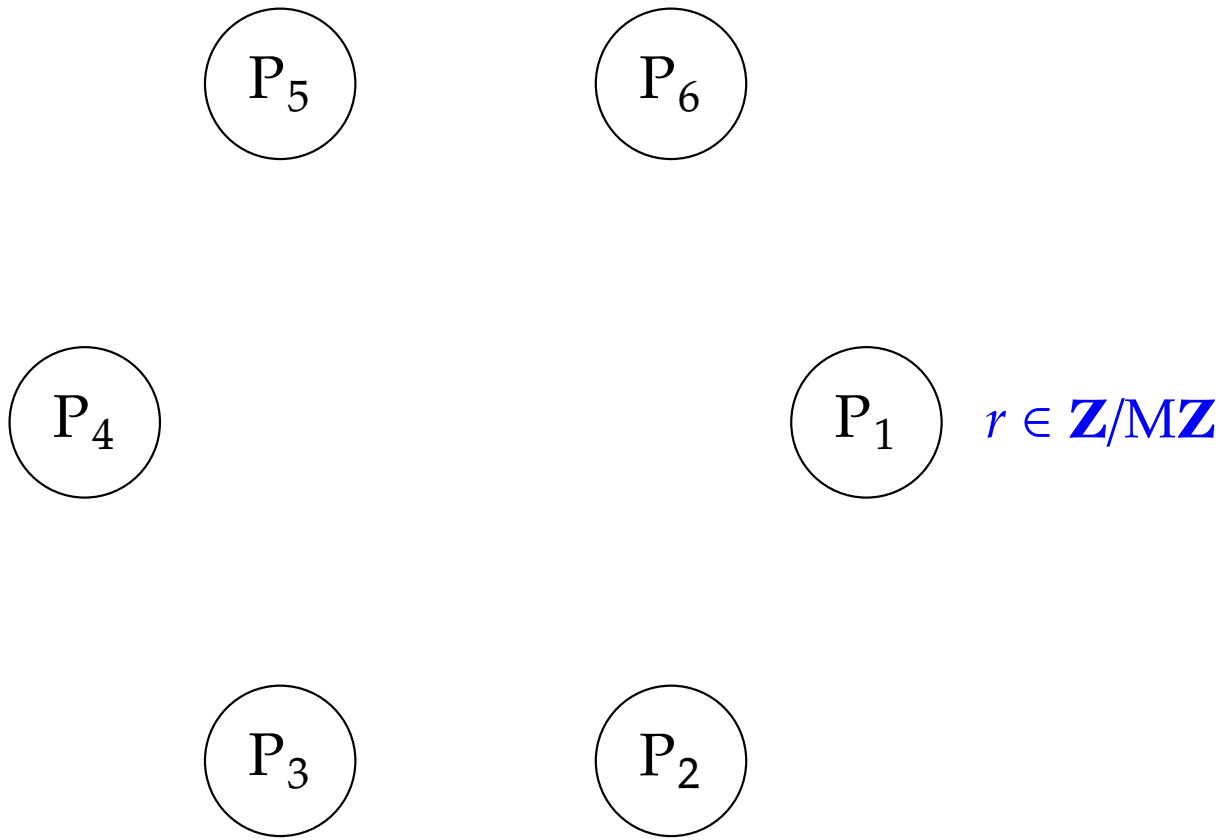
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



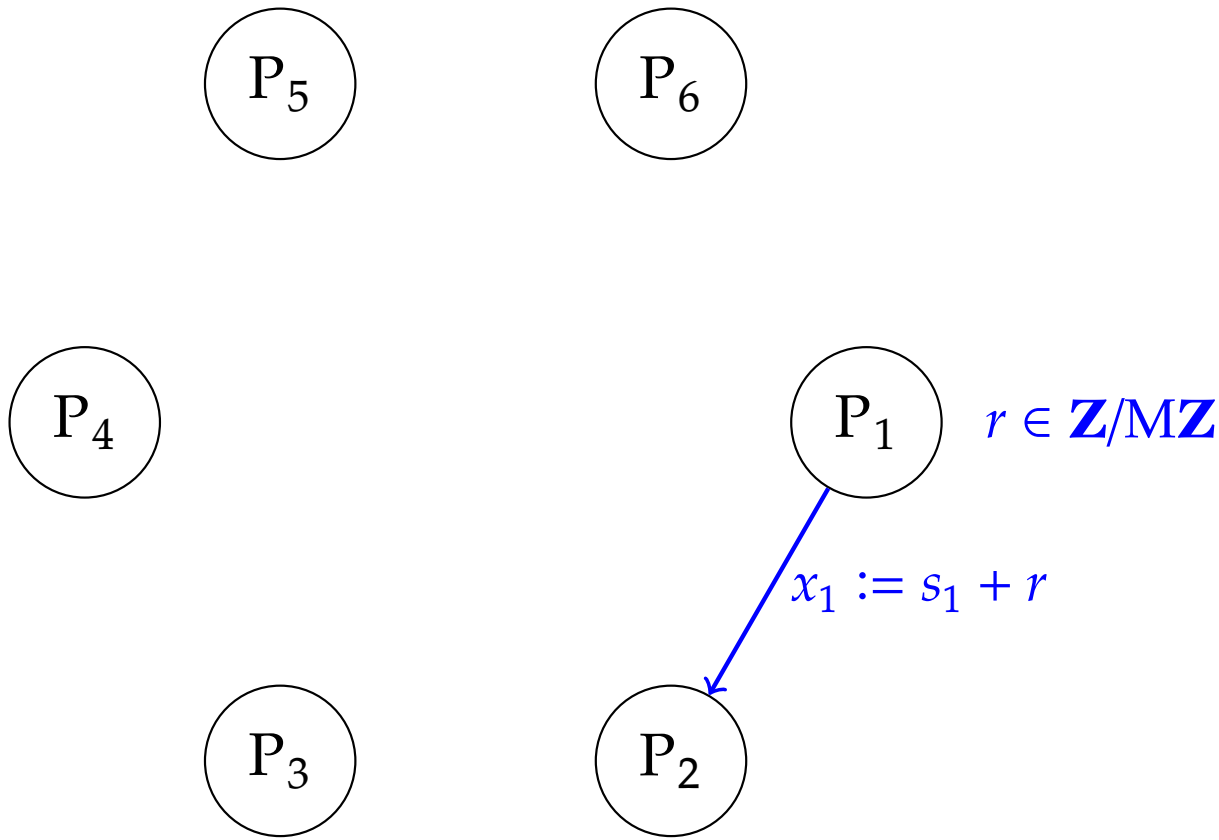
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



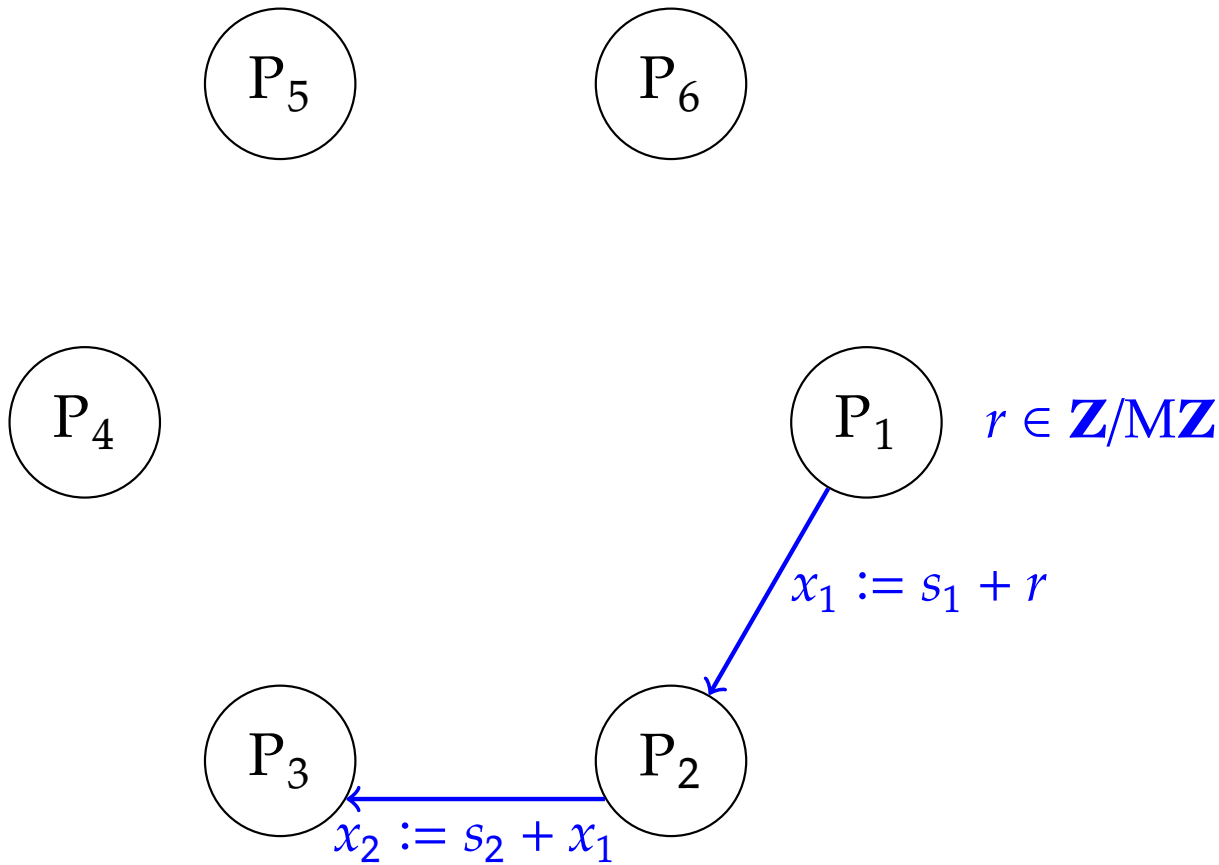
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



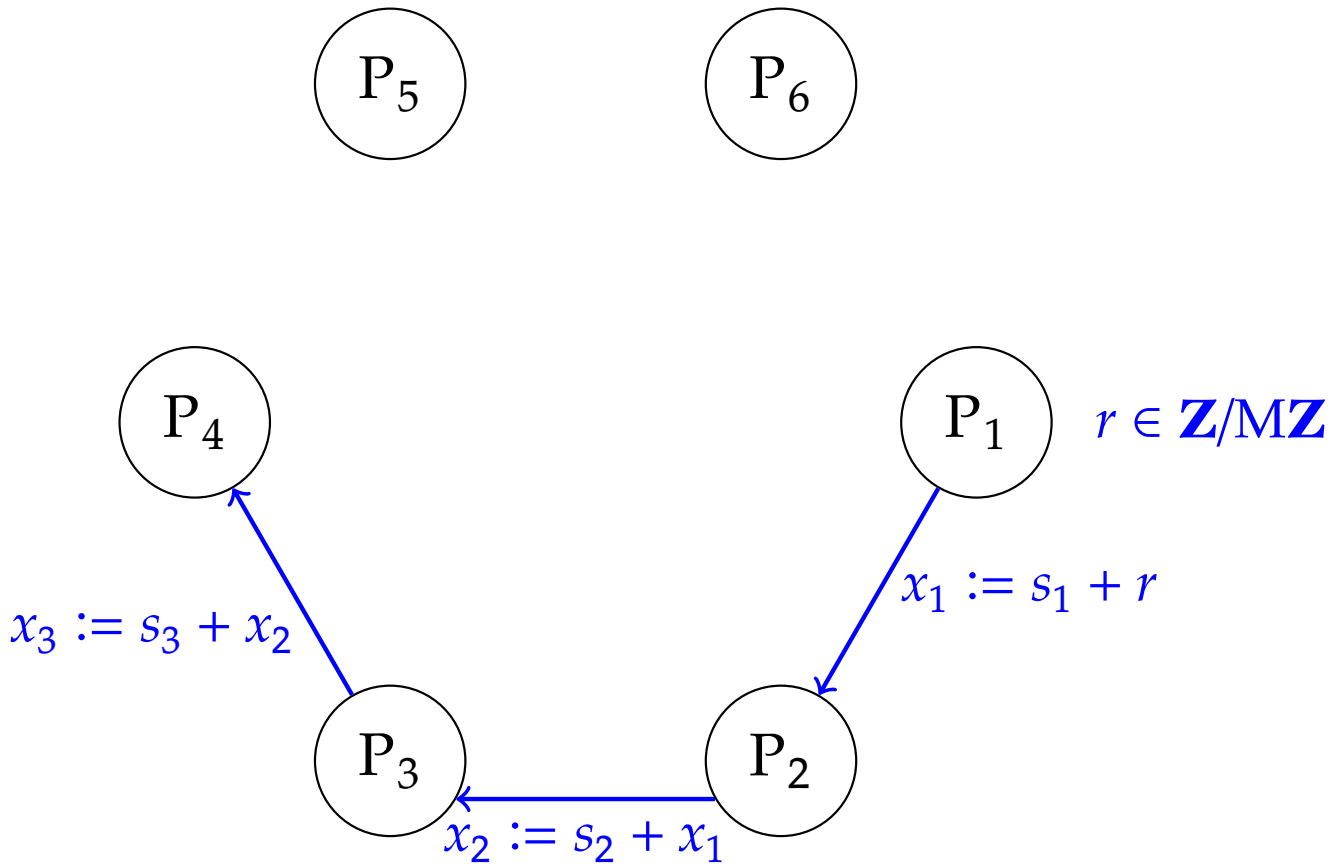
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



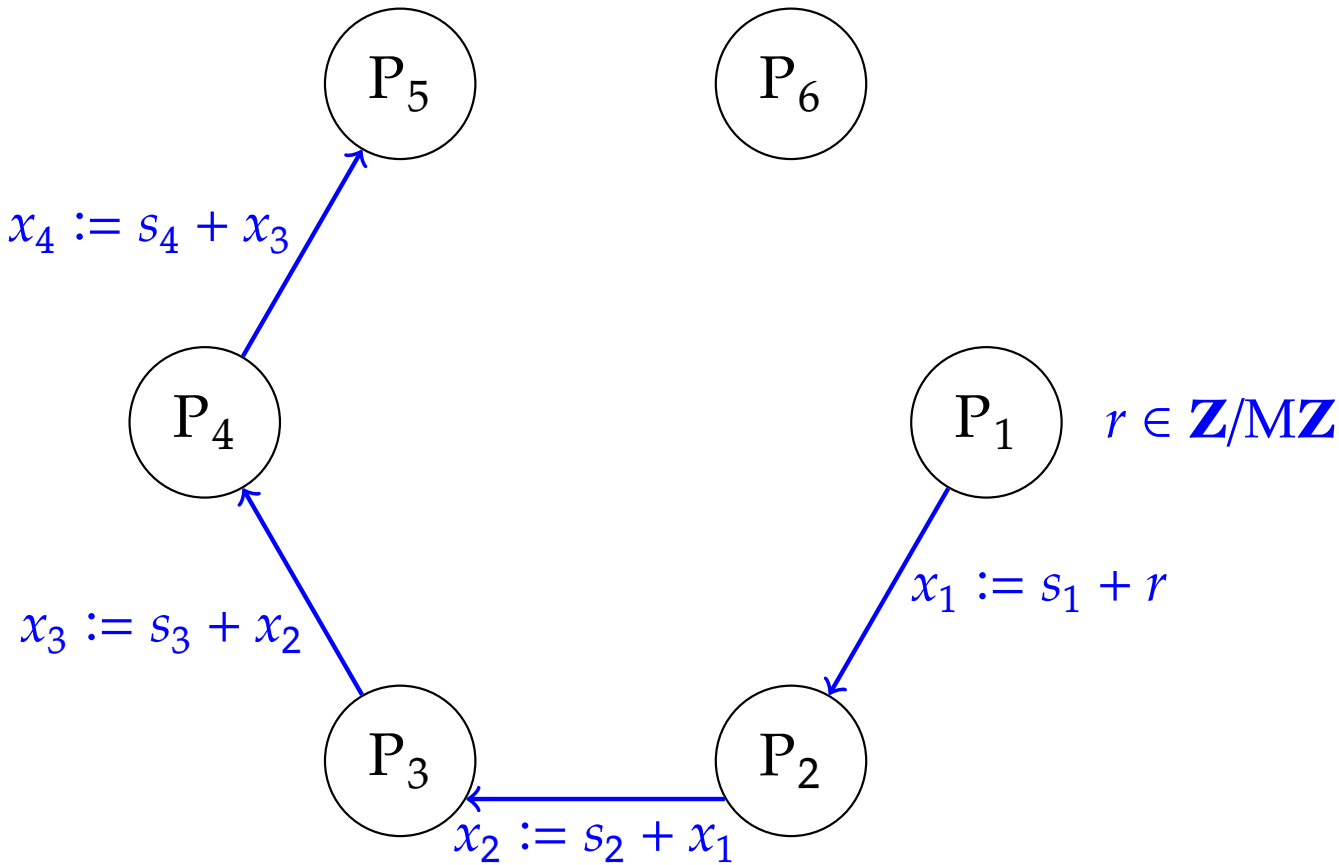
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



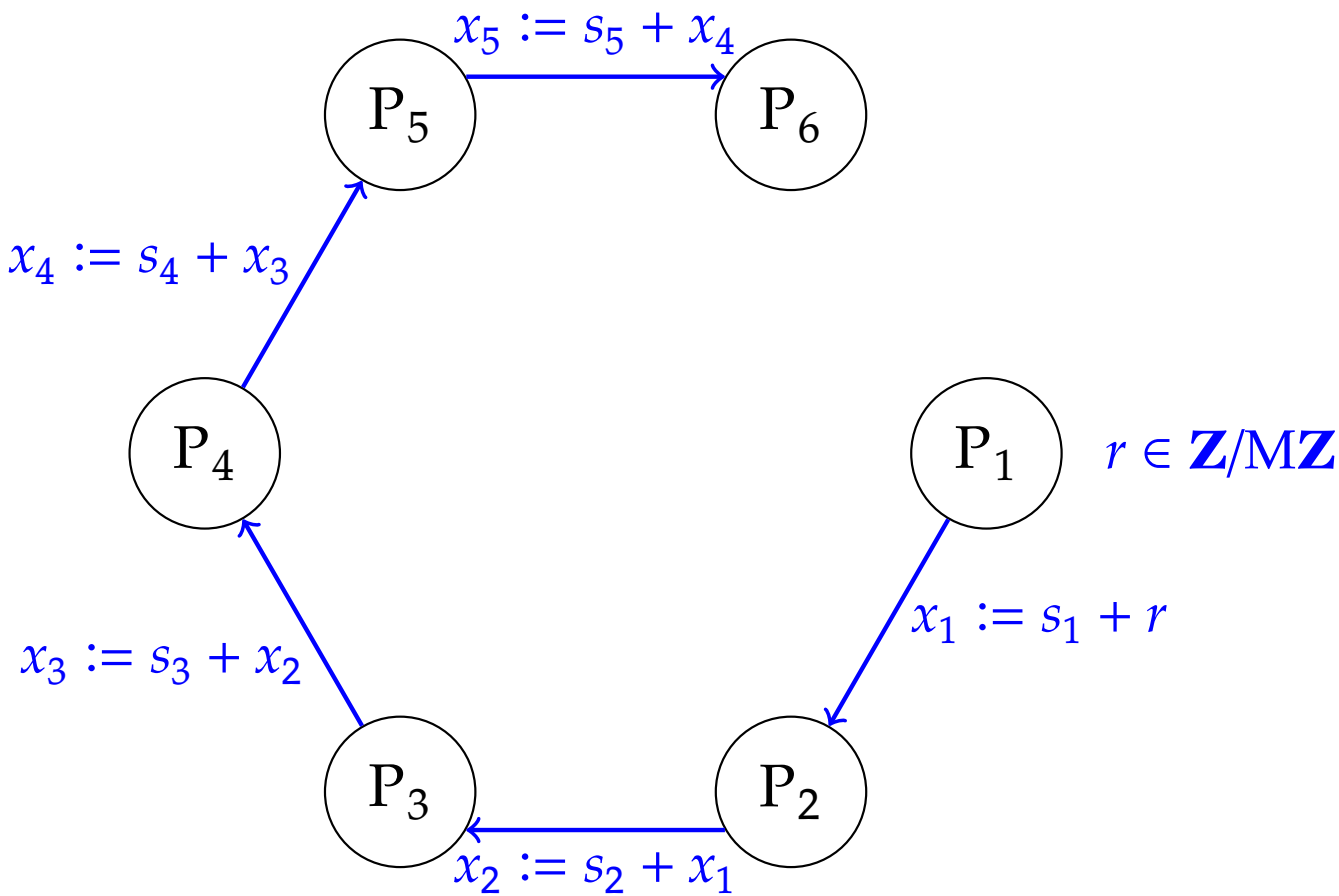
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



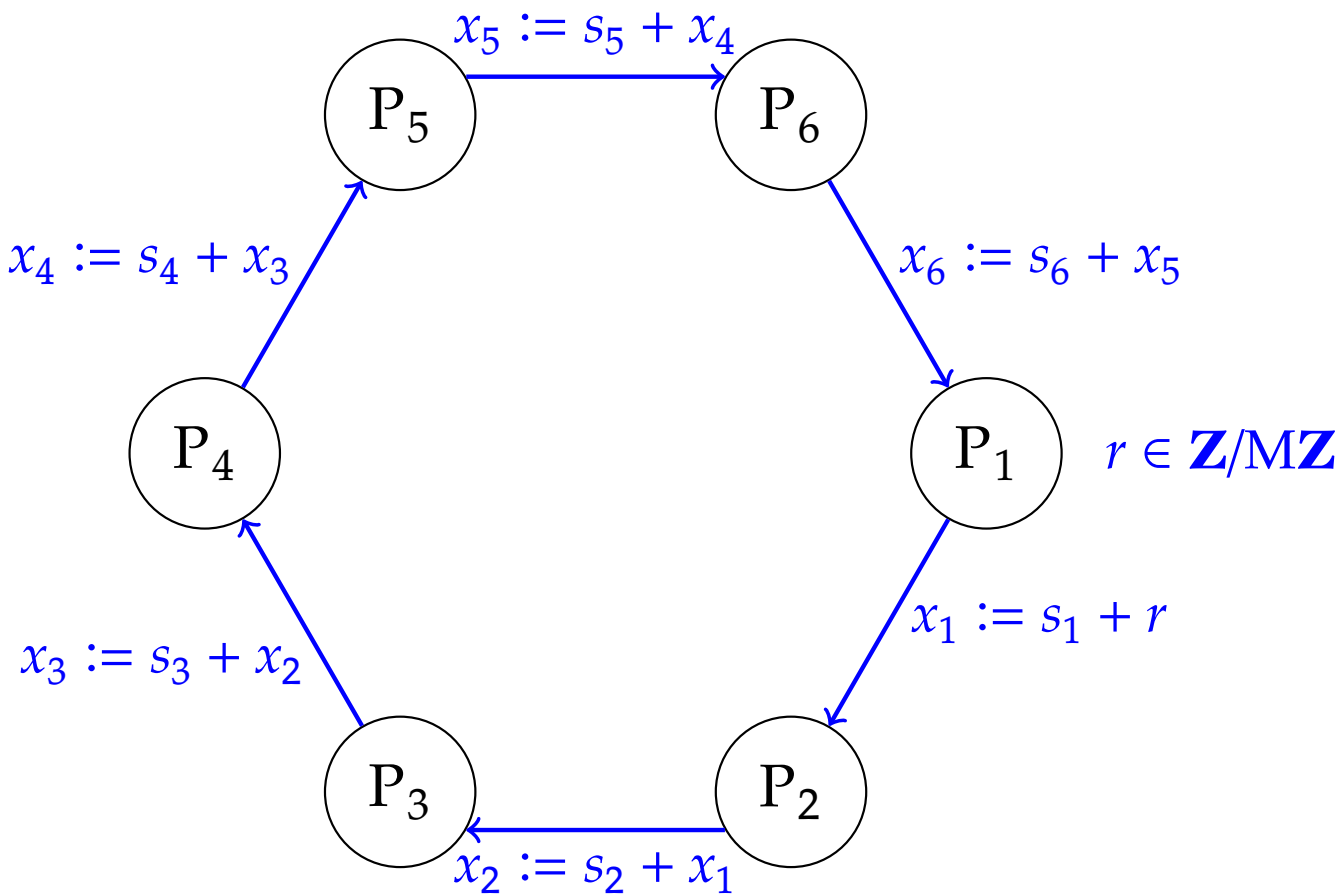
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



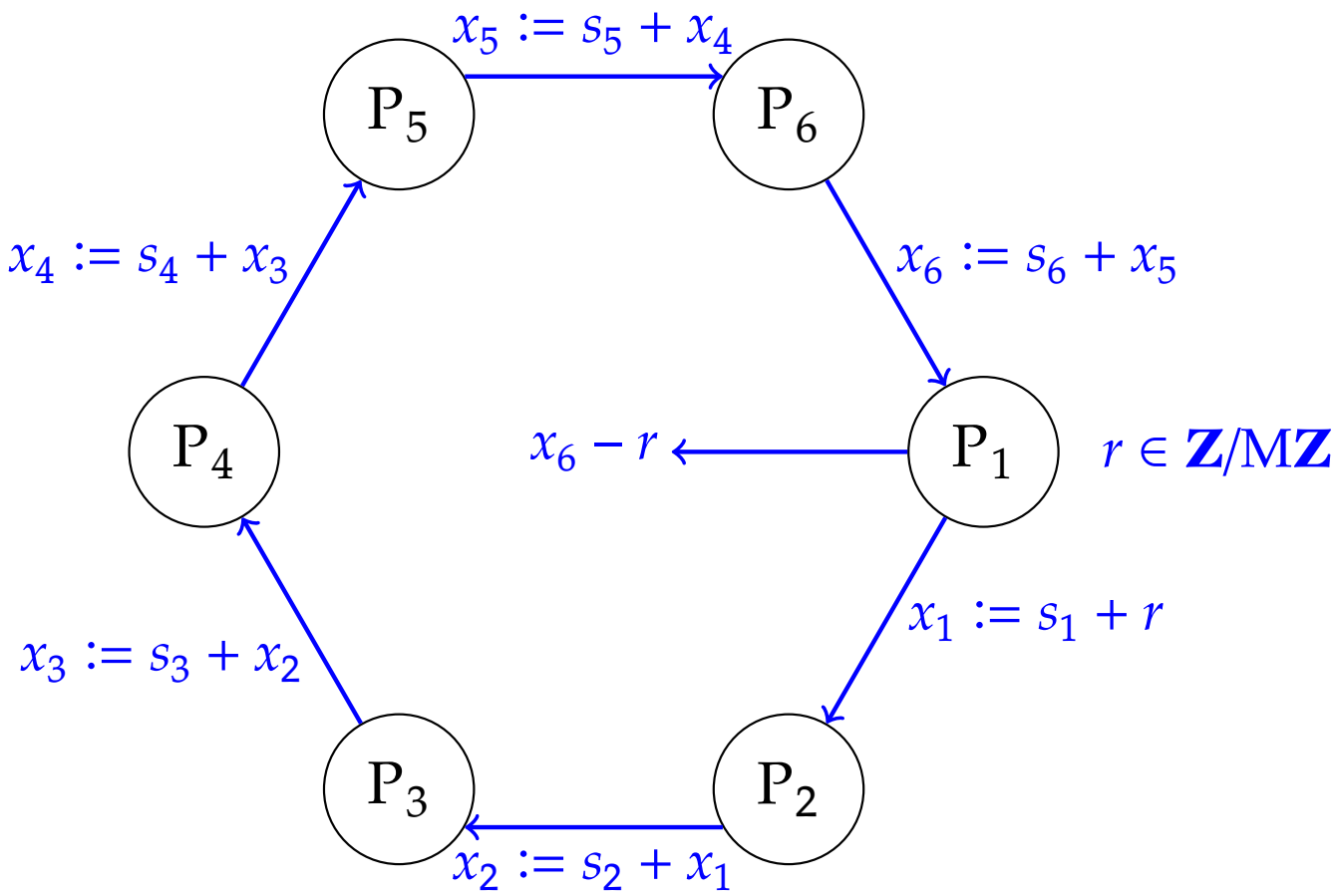
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



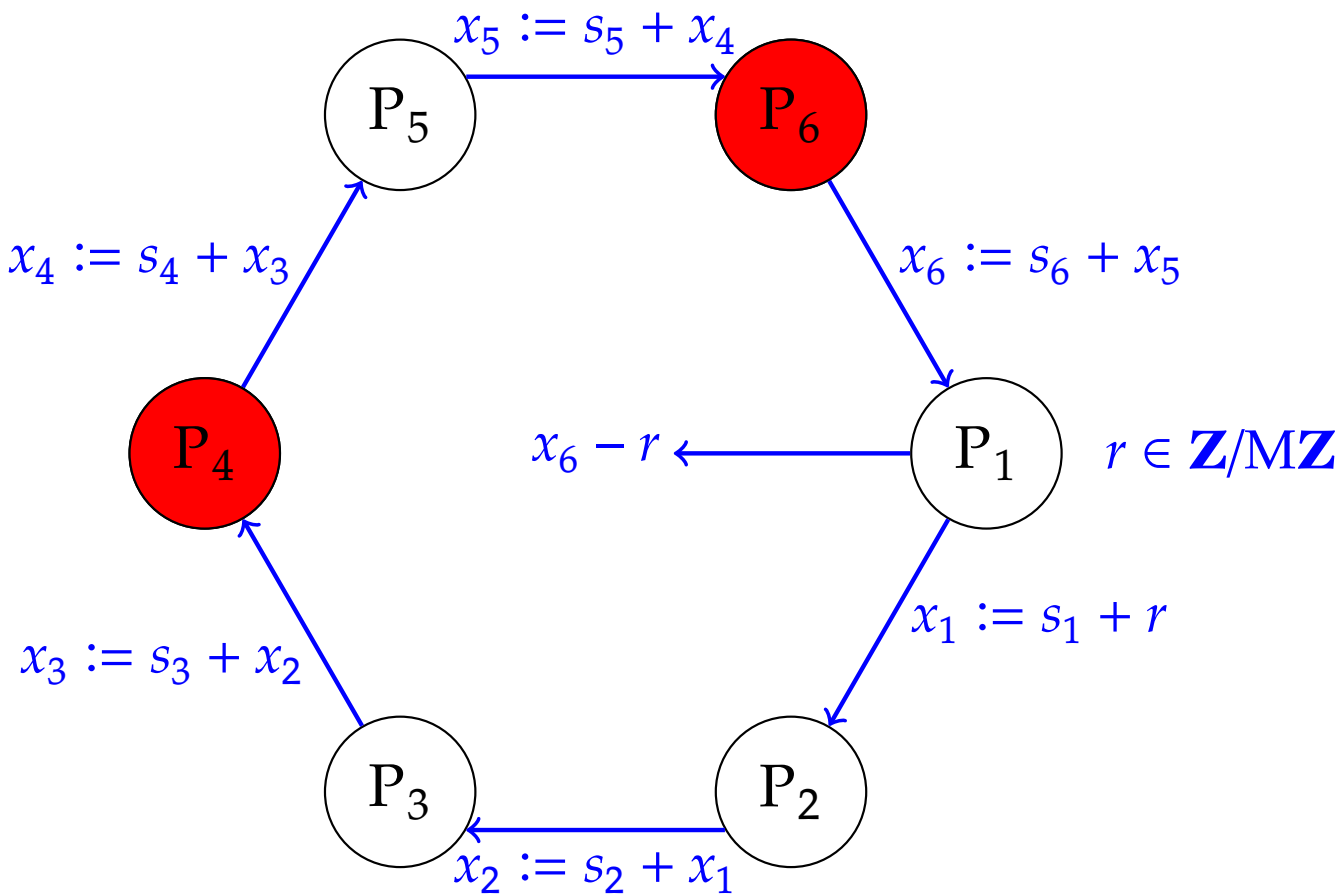
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



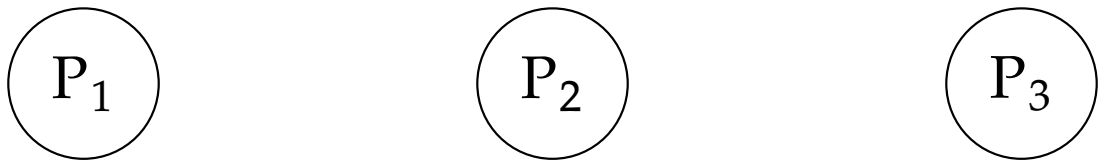
Exemple de la moyenne des salaires

- Chaque P_i a pour salaire $s_i \in \mathbf{N}$, avec $s_i < M$



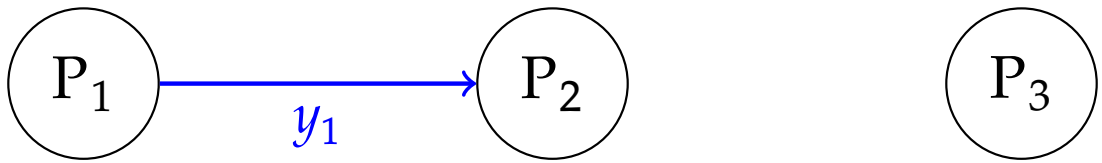
Exemple de la moyenne des salaires

- Chaque P_i prend au hasard $x_i, y_i, z_i \in \mathbf{Z}/M\mathbf{Z}$ tel que $s_i = x_i + y_i + z_i \in \mathbf{Z}/M\mathbf{Z}$ et distribue ses parts



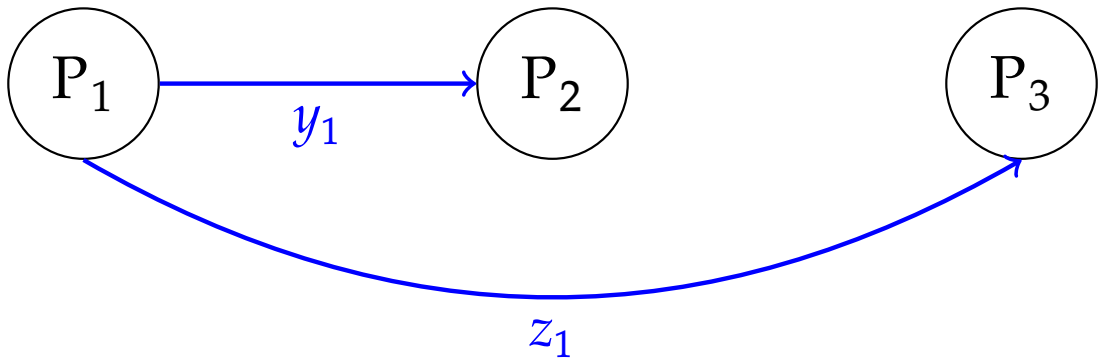
Exemple de la moyenne des salaires

- Chaque P_i prend au hasard $x_i, y_i, z_i \in \mathbf{Z}/M\mathbf{Z}$ tel que $s_i = x_i + y_i + z_i \in \mathbf{Z}/M\mathbf{Z}$ et distribue ses parts



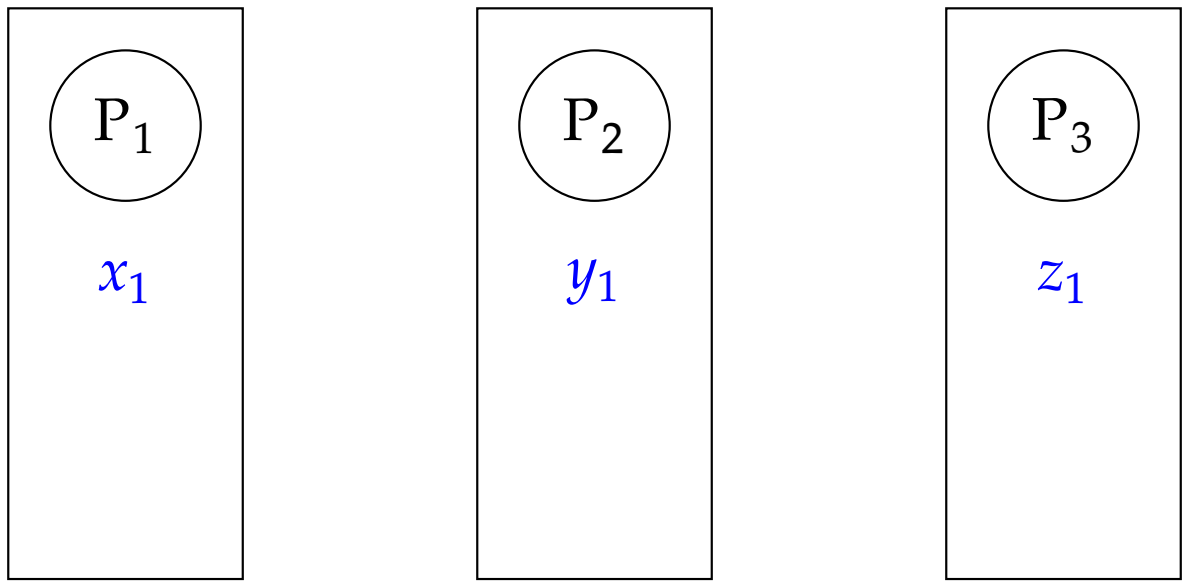
Exemple de la moyenne des salaires

- Chaque P_i prend au hasard $x_i, y_i, z_i \in \mathbf{Z}/M\mathbf{Z}$ tel que $s_i = x_i + y_i + z_i \in \mathbf{Z}/M\mathbf{Z}$ et distribue ses parts



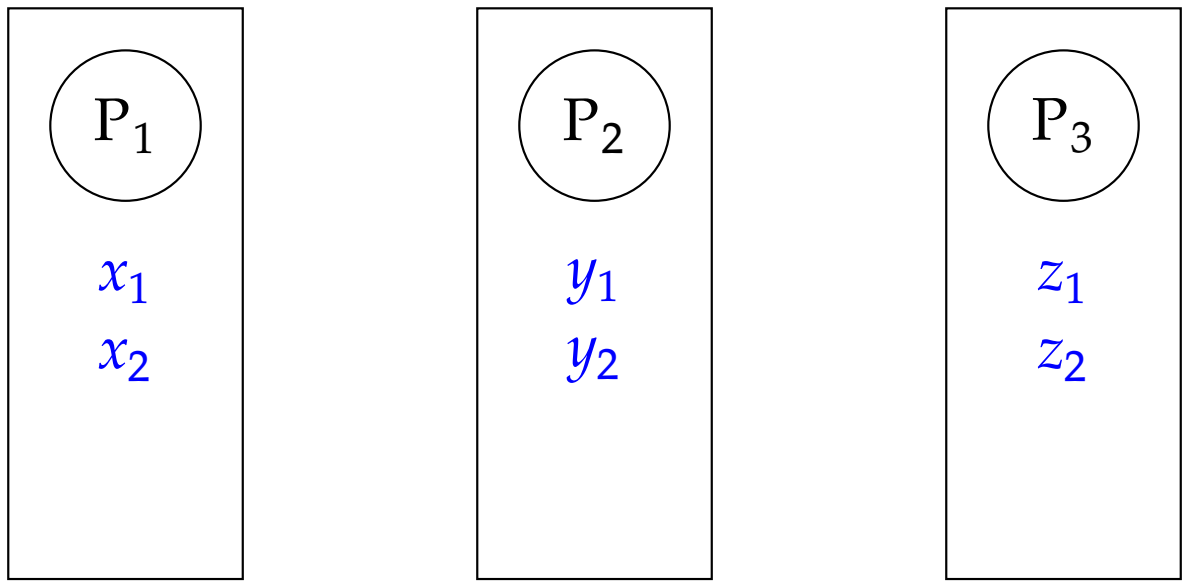
Exemple de la moyenne des salaires

- Chaque P_i prend au hasard $x_i, y_i, z_i \in \mathbf{Z}/M\mathbf{Z}$ tel que $s_i = x_i + y_i + z_i \in \mathbf{Z}/M\mathbf{Z}$ et distribue ses parts



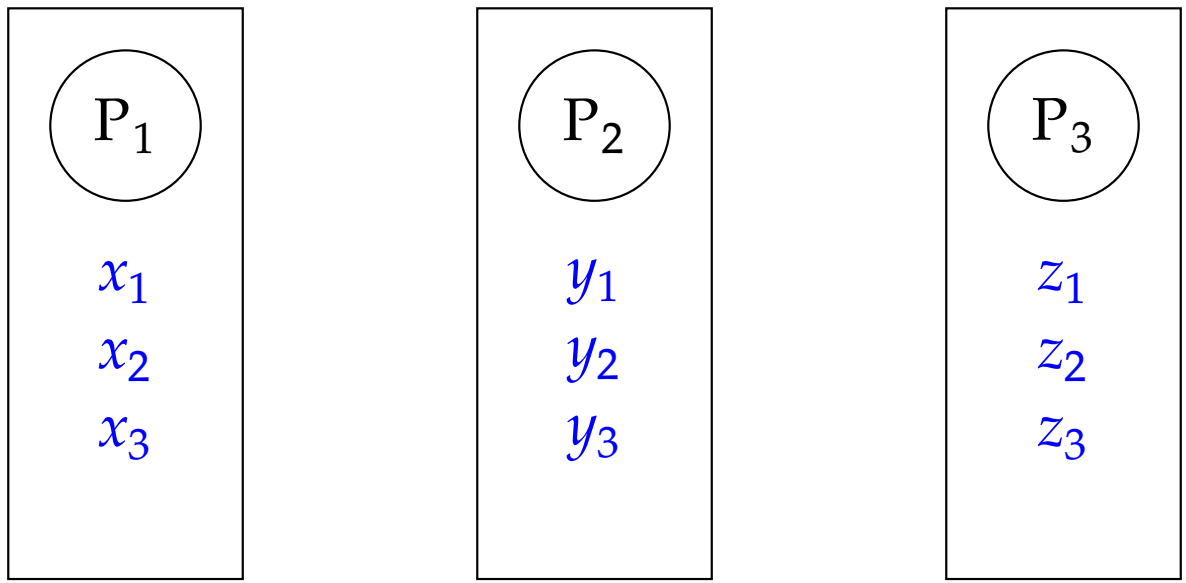
Exemple de la moyenne des salaires

- Chaque P_i prend au hasard $x_i, y_i, z_i \in \mathbf{Z}/M\mathbf{Z}$ tel que $s_i = x_i + y_i + z_i \in \mathbf{Z}/M\mathbf{Z}$ et distribue ses parts



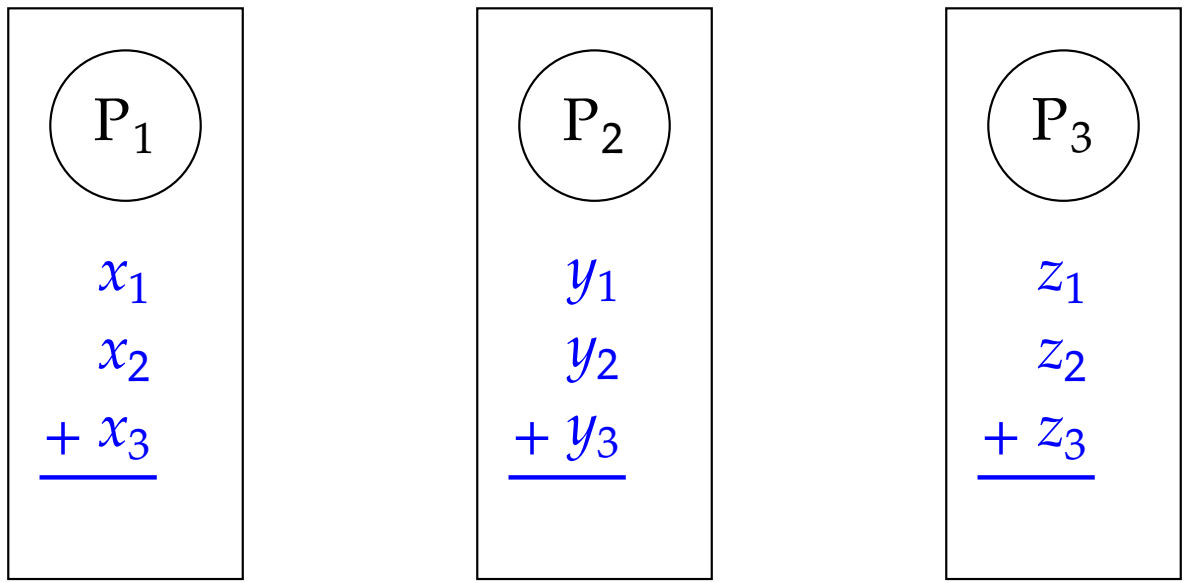
Exemple de la moyenne des salaires

- Chaque P_i prend au hasard $x_i, y_i, z_i \in \mathbf{Z}/M\mathbf{Z}$ tel que $s_i = x_i + y_i + z_i \in \mathbf{Z}/M\mathbf{Z}$ et distribue ses parts



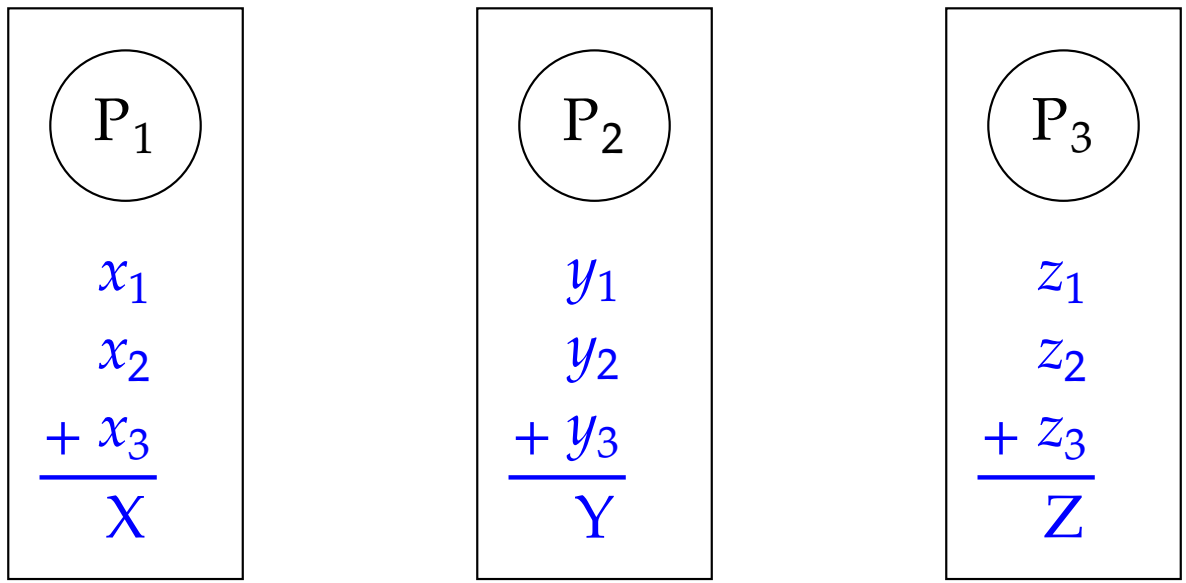
Exemple de la moyenne des salaires

- Chaque P_i prend au hasard $x_i, y_i, z_i \in \mathbf{Z}/M\mathbf{Z}$ tel que $s_i = x_i + y_i + z_i \in \mathbf{Z}/M\mathbf{Z}$ et distribue ses parts



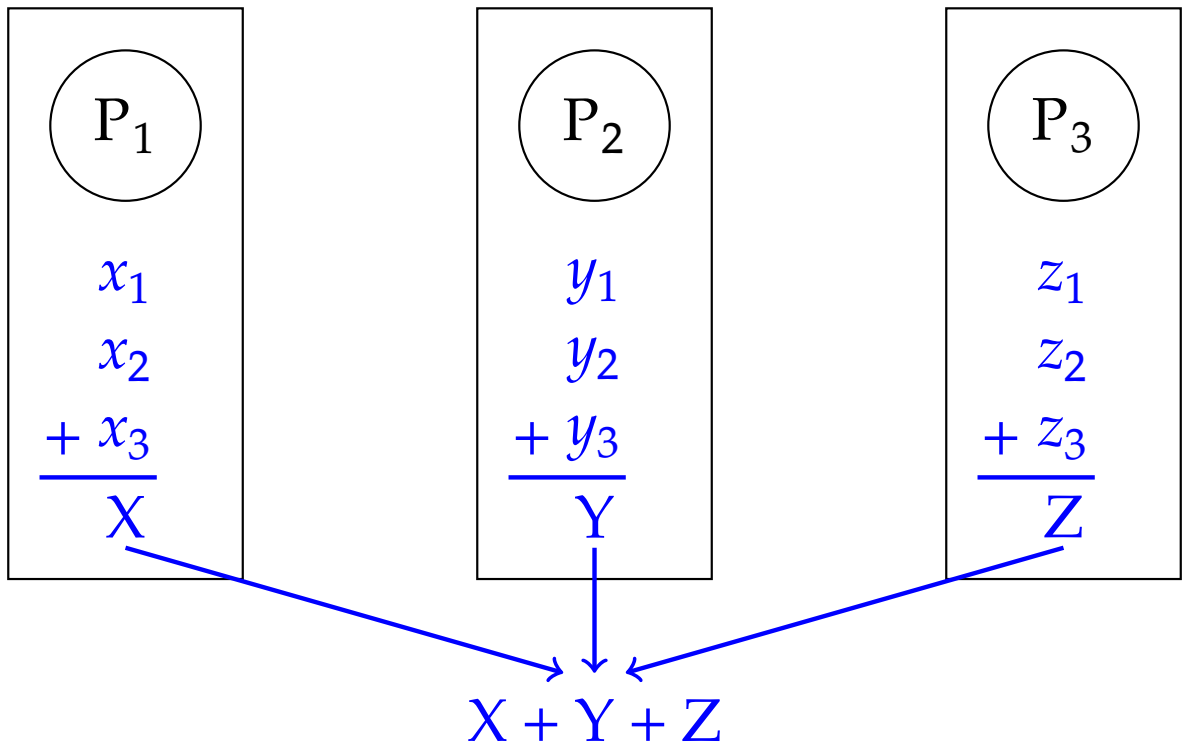
Exemple de la moyenne des salaires

- Chaque P_i prend au hasard $x_i, y_i, z_i \in \mathbf{Z}/M\mathbf{Z}$ tel que $s_i = x_i + y_i + z_i \in \mathbf{Z}/M\mathbf{Z}$ et distribue ses parts



Exemple de la moyenne des salaires

- Chaque P_i prend au hasard $x_i, y_i, z_i \in \mathbf{Z}/M\mathbf{Z}$ tel que $s_i = x_i + y_i + z_i \in \mathbf{Z}/M\mathbf{Z}$ et distribue ses parts



Et le RDV d'Alice et Bob ?

- Alice a un bit secret $a \in \{0,1\}$
- Bob a un bit secret $b \in \{0,1\}$
- Ils veulent calculer

$$f(a,b) = a \text{ ET } b$$

Ingrédients

- Un système de chiffrement avec des propriétés homomorphes
  - Par exemple :

$$c := \mathrm{E}(m)\mathrm{E}(m')$$

  - En déchiffrant c on obtient mm'
  - RSA : $\mathrm{E}(m) = m^e \mod \mathrm{N}$
- Un protocole de transfert inconscient

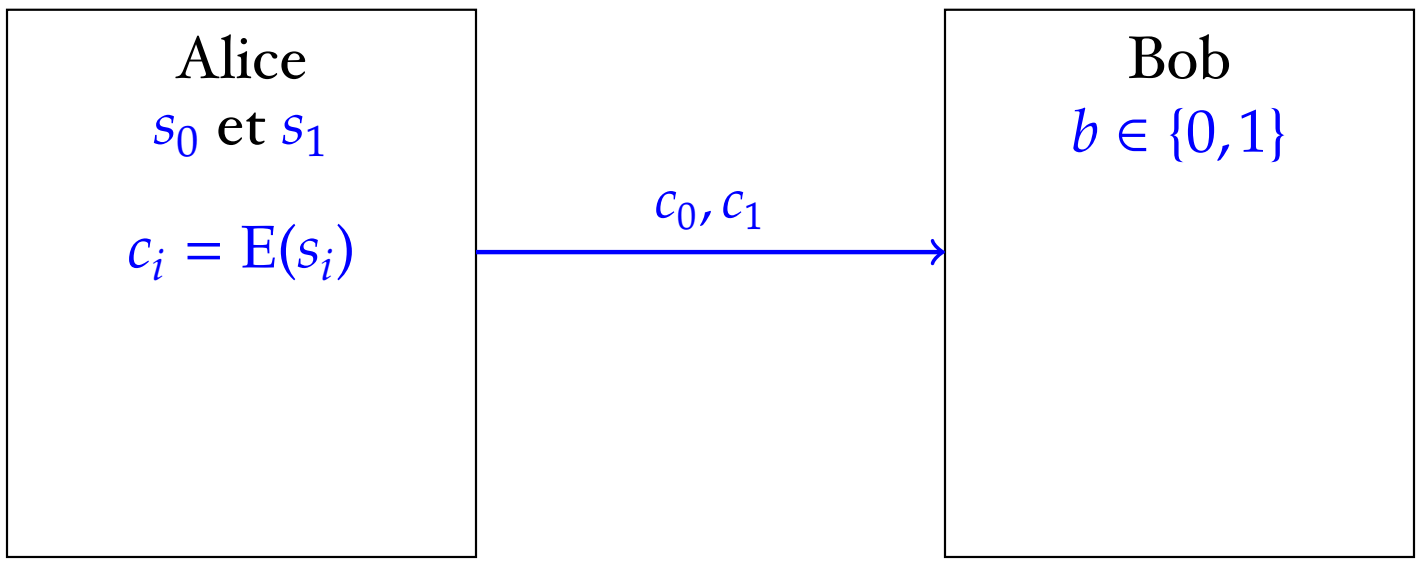
Alice	Bob
s_0 et s_1	$b \in \{0,1\}$

Ingrédients

- Un système de chiffrement avec des propriétés homomorphes
  - Par exemple :

$$c := \mathrm{E}(m)\mathrm{E}(m')$$

  - En déchiffrant c on obtient mm'
  - RSA : $\mathrm{E}(m) = m^e \mod \mathrm{N}$
- Un protocole de transfert inconscient

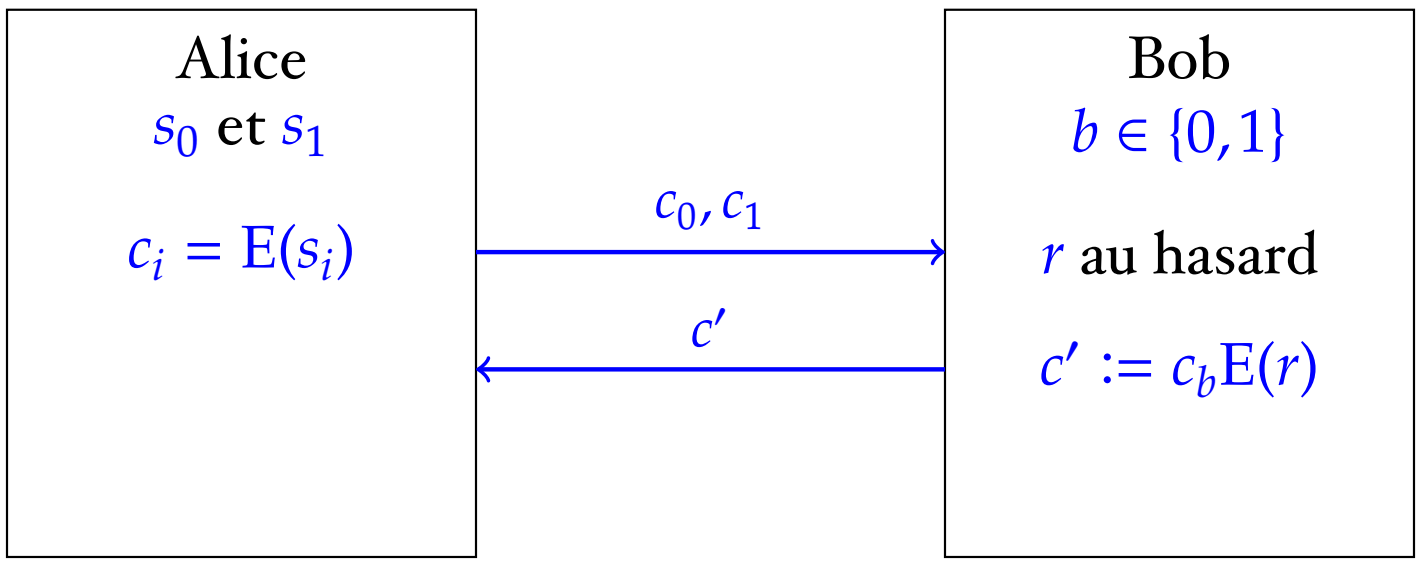


Ingrédients

- Un système de chiffrement avec des propriétés homomorphes
  - Par exemple :

$$c := \mathrm{E}(m)\mathrm{E}(m')$$

  - En déchiffrant c on obtient mm'
  - RSA : $\mathrm{E}(m) = m^e \mod \mathrm{N}$
- Un protocole de transfert inconscient

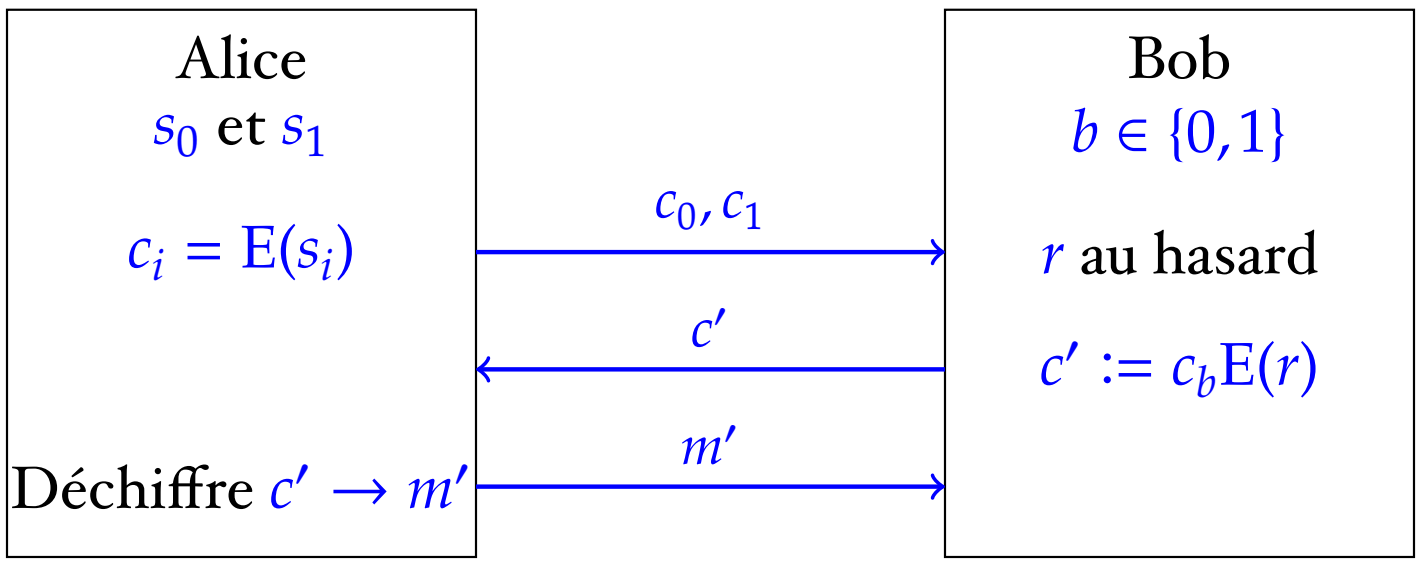


Ingrédients

- Un système de chiffrement avec des propriétés homomorphes
  - Par exemple :

$$c := \mathrm{E}(m)\mathrm{E}(m')$$

  - En déchiffrant c on obtient mm'
  - RSA : $\mathrm{E}(m) = m^e \mod \mathrm{N}$
- Un protocole de transfert inconscient

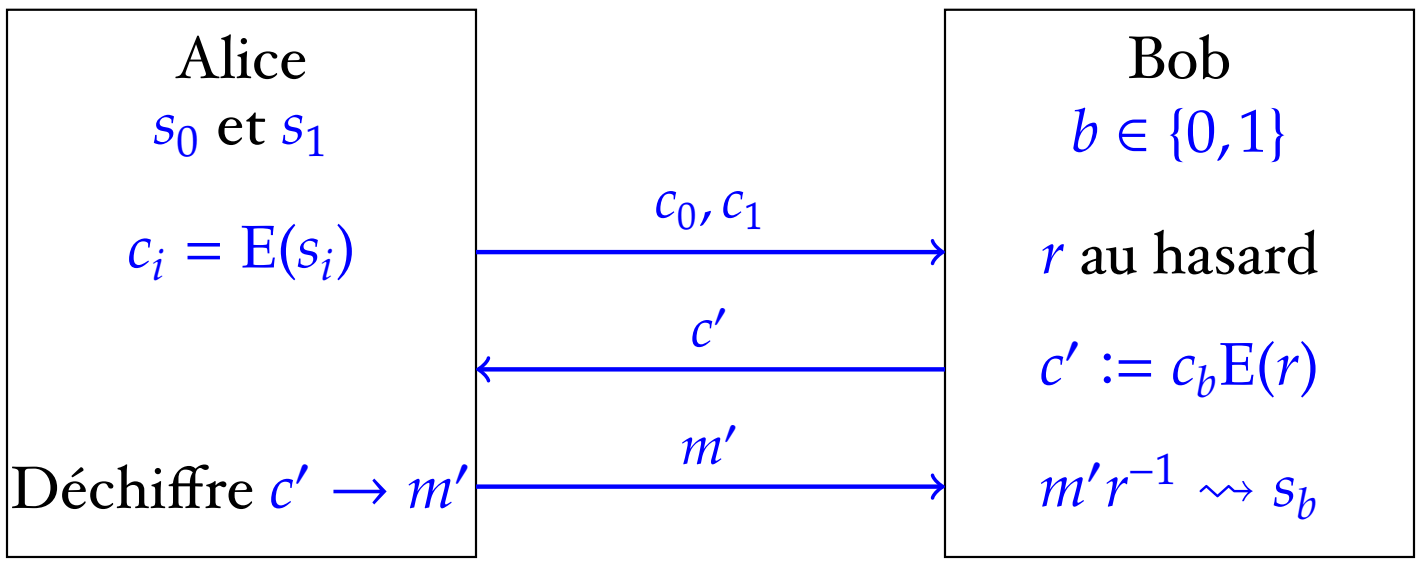


Ingrédients

- Un système de chiffrement avec des propriétés homomorphes
  - Par exemple :

$$c := \mathrm{E}(m)\mathrm{E}(m')$$

  - En déchiffrant c on obtient mm'
  - RSA : $\mathrm{E}(m) = m^e \mod \mathrm{N}$
- Un protocole de transfert inconscient



Le protocole

- Alice a un bit secret $a \in \{0,1\}$
- Bob a un bit secret $b \in \{0,1\}$
- Ils utilisent le transfert inconscient :
- Si $a = 0$
  - Alice pose $s_0 = s_1 = 0$
  - Bob récupère s_b et le renvoie à Alice
- Si $a = 1$
  - Alice pose $s_0 = 0$ et $s_1 = 1$
  - Bob récupère s_b et le renvoie à Alice

Cas général

- Avec n utilisateurs dont t sont malveillants
- Plusieurs résultats théoriques (fin des années 80) : toute fonction f peut être calculée
  - Si $t < n/2$ (la majorité est honnête)
  - Si $t < n$ avec des hypothèses et certaines restrictions
- Ingrédients :
  - Transfert inconscient
  - Partage de secret
  - Chiffrement homomorphe
  - Preuve à divulgation nulle de connaissance
  - ...

Ces dernières années

- Beaucoup d'avancées sur l'efficacité des solutions
- Secteurs en vogue, nombreuses startups sur le sujet
- Exemples d'utilisations « grandeur nature » :
  - Calcul de l'écart salarial homme femme dans la région de Boston (2017)
  - Calcul du taux de conversion publicitaire par Google
  - Partage de clefs cryptographiques (signatures de transactions Bitcoin)

Questions ?