

Multi-Party Computation (Cálculo Seguro Multipartito)

CatíoCrypto

Eduardo Soria Vázquez
eduardo.soria-vazquez@tii.ae

I ¿De qué se ocupa la criptografía?

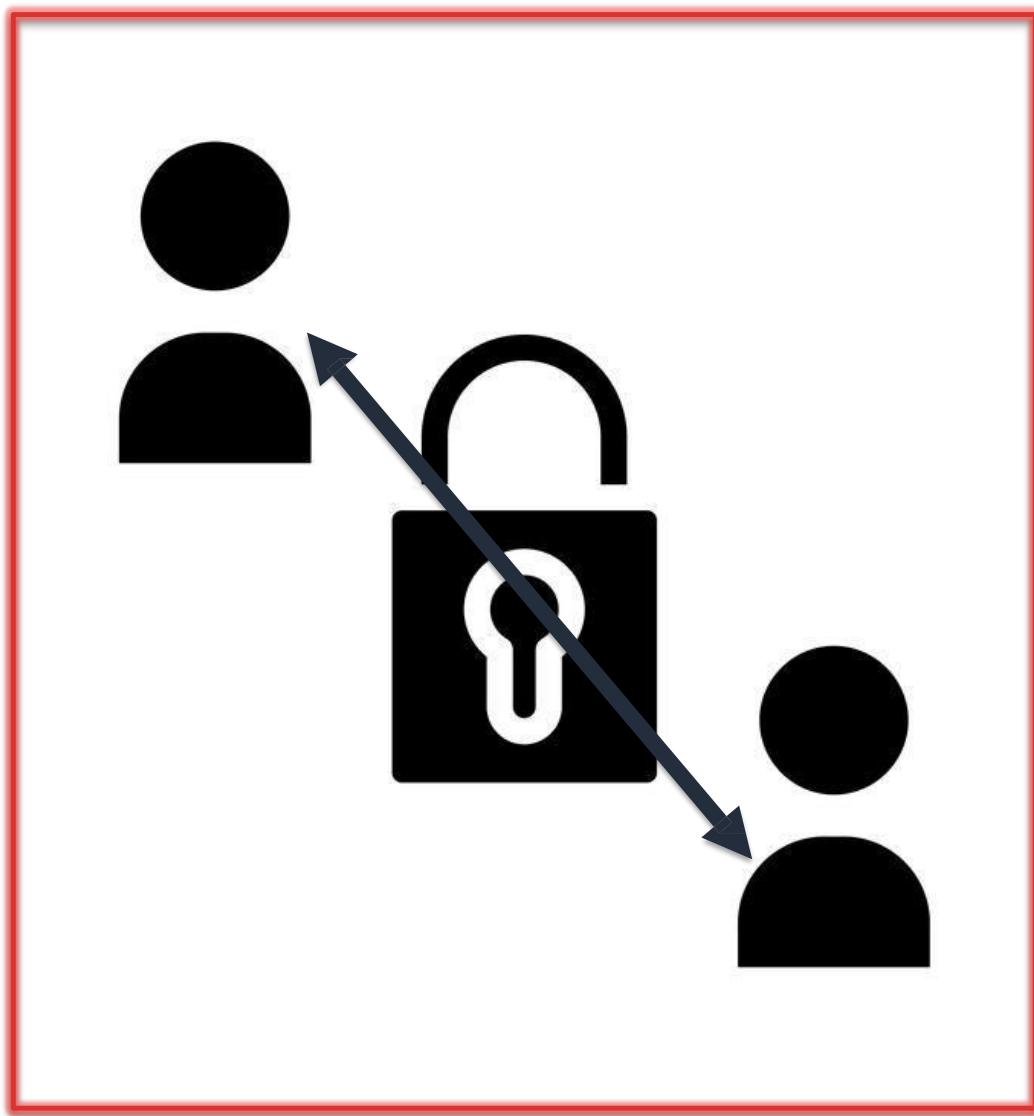
“Cryptography rearranges power: it configures who can do what, from what.”

Phillip Rogaway, “The moral character of cryptographic work”.

- Verifiable Computation / Cálculo verificable (VC): Demostrar que se ha ejecutado un programa, sin que quien lo verifique tenga que re-ejecutarlo.
- Zero-Knowledge Proofs / Pruebas de conocimiento nulo (ZK): Similar a VC, pero quien demuestra hacer el cálculo puede mantener algunos datos ocultos.
- Secret Sharing / Repartición de secretos: Fragmentar un secreto entre varias entidades, de tal forma que solo pueda reconstruirse si ciertos subconjuntos de ellas acuerdan hacerlo.
- Multi-Party Computation (MPC): Calcular sobre datos “sin verlos”, de forma distribuida.
- ¡Mucho más!! Privacidad Diferencial (DP), Recuperación privada de información (PIR), Cifrado totalmente homomórfico (FHE), Cifrado funcional (FE), Time-Lock Puzzles, Blockchains, Criptomonedas...

I Introducción

Comunicación segura Almacenamiento seguro



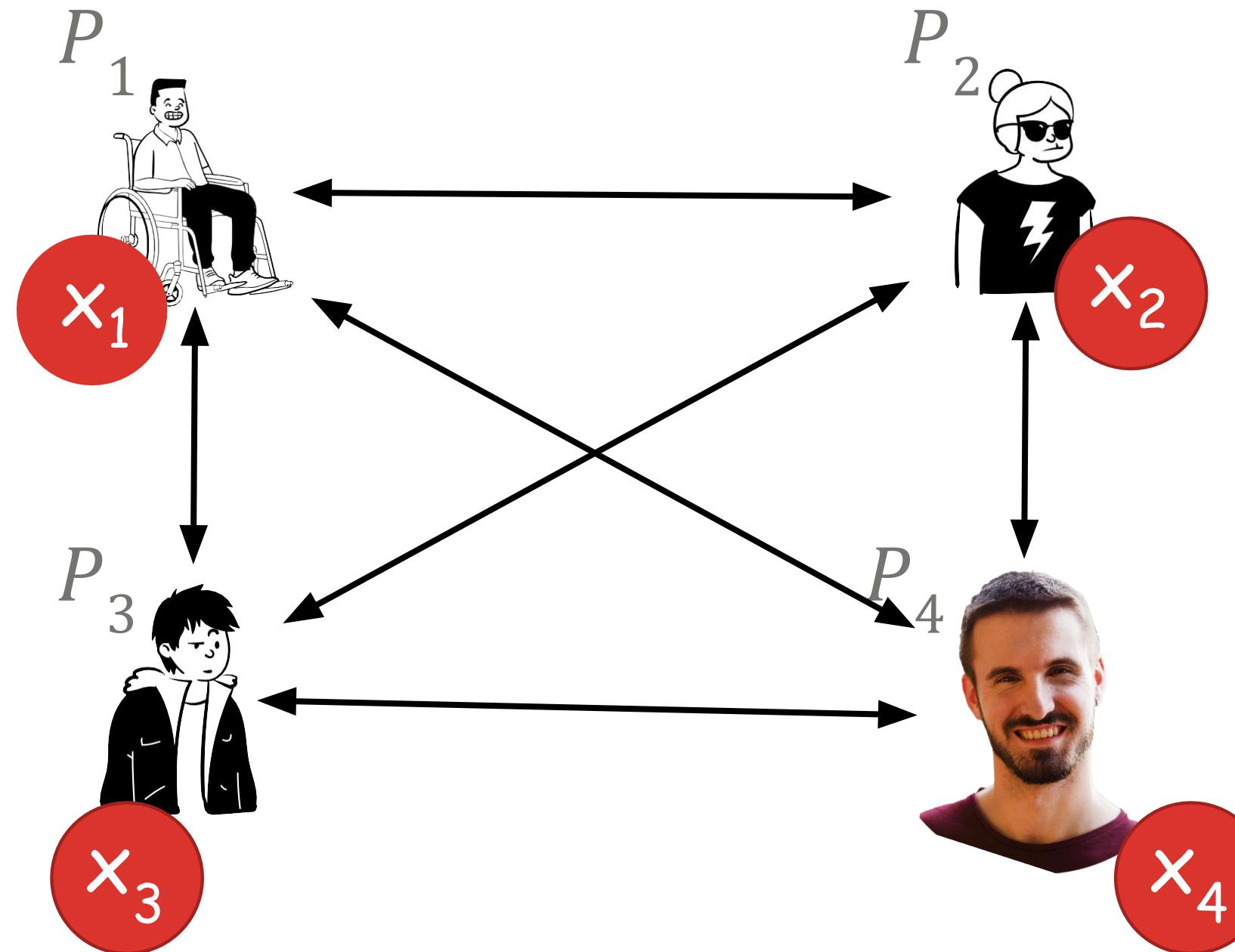
Cálculo Seguro



Criptografía Clásica

Multi-Party Computation,
Cifrado Homomórfico...

Introducción: Multi-Party Computation (MPC)

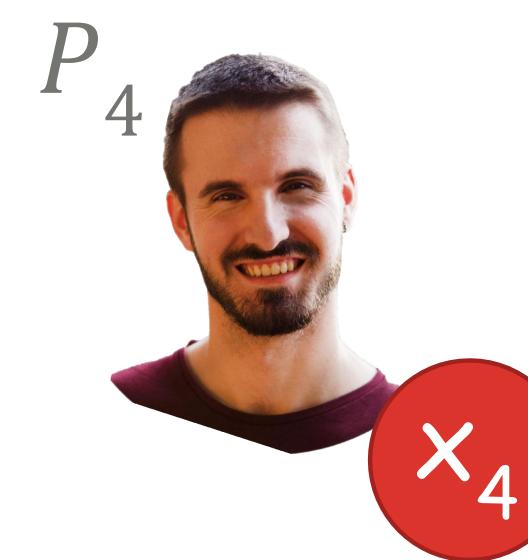
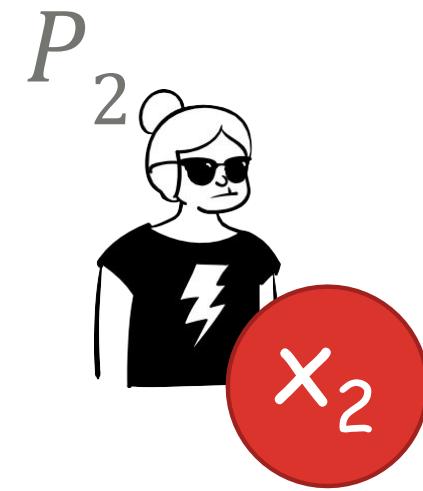


$$y = f(x_1, x_2, x_3, x_4)$$

Un protocolo de MPC consta de:

- n entidades que “desconfían” las unas de las otras.
- Cada entidad P_i puede aportar inputs secretos.
- **Objetivo:** Calcular una función (pública) sobre el conjunto de sus datos privados. Con las garantías de:
 - No revelar nada más que el resultado de la función.
 - ... y otras muchas.

Introducción: Multi-Party Computation (MPC)

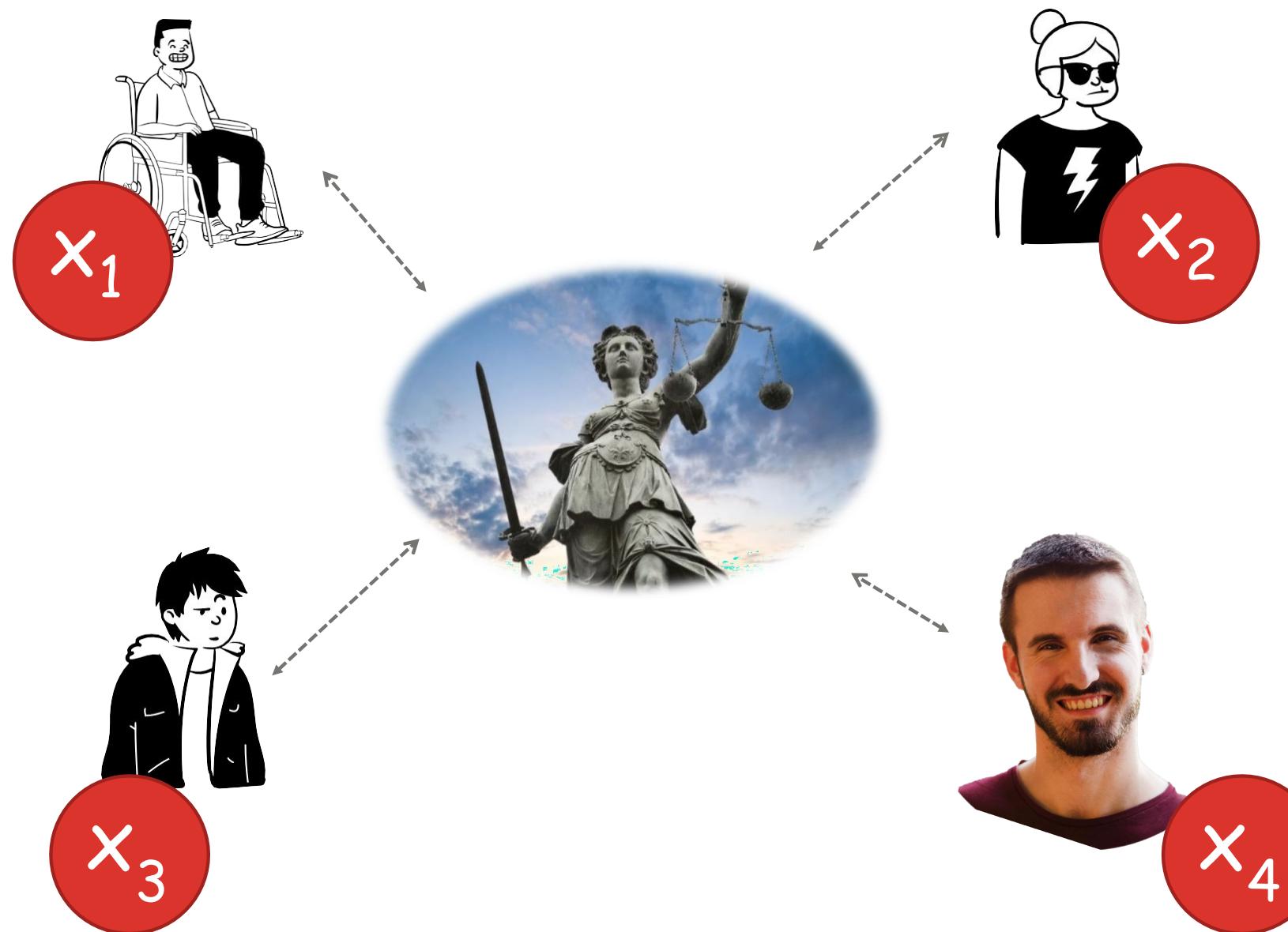


$$y = f(x_1, x_2, x_3, x_4)$$

Un protocolo de MPC consta de:

- n entidades que “desconfían” las unas de las otras.
- Cada entidad P_i puede aportar inputs secretos.
- **Objetivo:** Calcular una función (pública) sobre el conjunto de sus datos privados. Con las garantías de:
 - No revelar nada más que el resultado de la función.
 - ... y otras muchas.

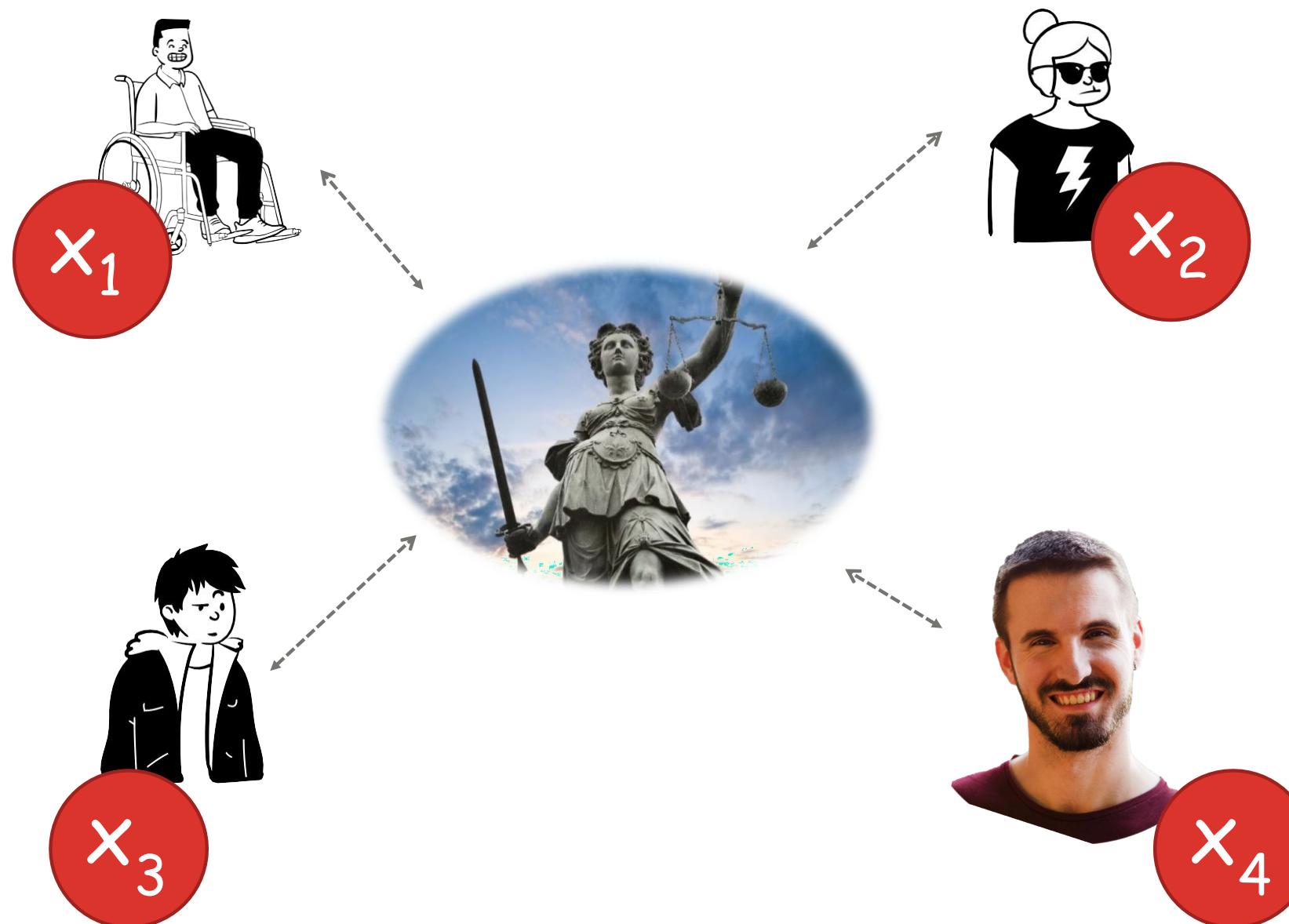
Multi-Party Computation vs Tercera Parte de Confianza



Si hay una entidad en la cual TODOS confiamos, no hay necesidad de utilizar criptografía.

$$y = f(x_1, x_2, x_3, x_4)$$

Multi-Party Computation vs Tercera Parte de Confianza



$$y = f(x_1, x_2, x_3, x_4)$$

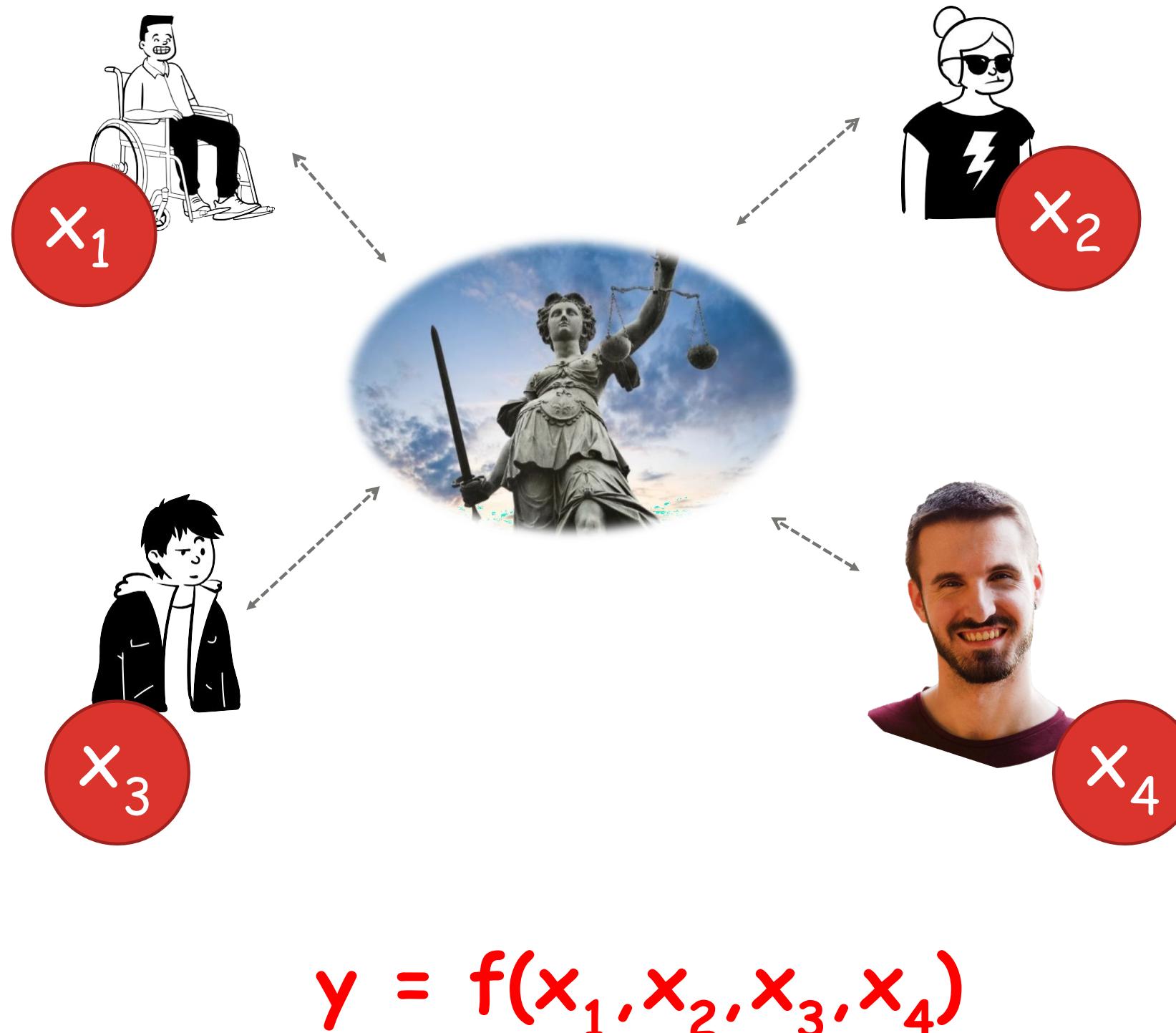
Si hay una entidad en la cual **TODOS confiamos**, no hay necesidad de utilizar criptografía.

Confiamos en que esta entidad nos garantice que:

- No revela nuestros datos a nadie más.
- Realiza el cálculo de forma correcta.
- No es susceptible a ser coaccionada, ni hackeada.
- Nos devuelve el mismo resultado a todos.
- Nos devuelve siempre el resultado.

...

Multi-Party Computation vs Tercera Parte de Confianza



Si hay una entidad en la cual **TODOS confiamos**, no hay necesidad de utilizar criptografía.

Confiamos en que esta entidad nos garantice que:

- No revela nuestros datos a nadie más.
- Realiza el cálculo de forma correcta.
- No es susceptible a ser coaccionada, ni hackeada.
- Nos devuelve el mismo resultado a todos.
- Nos devuelve siempre el resultado.

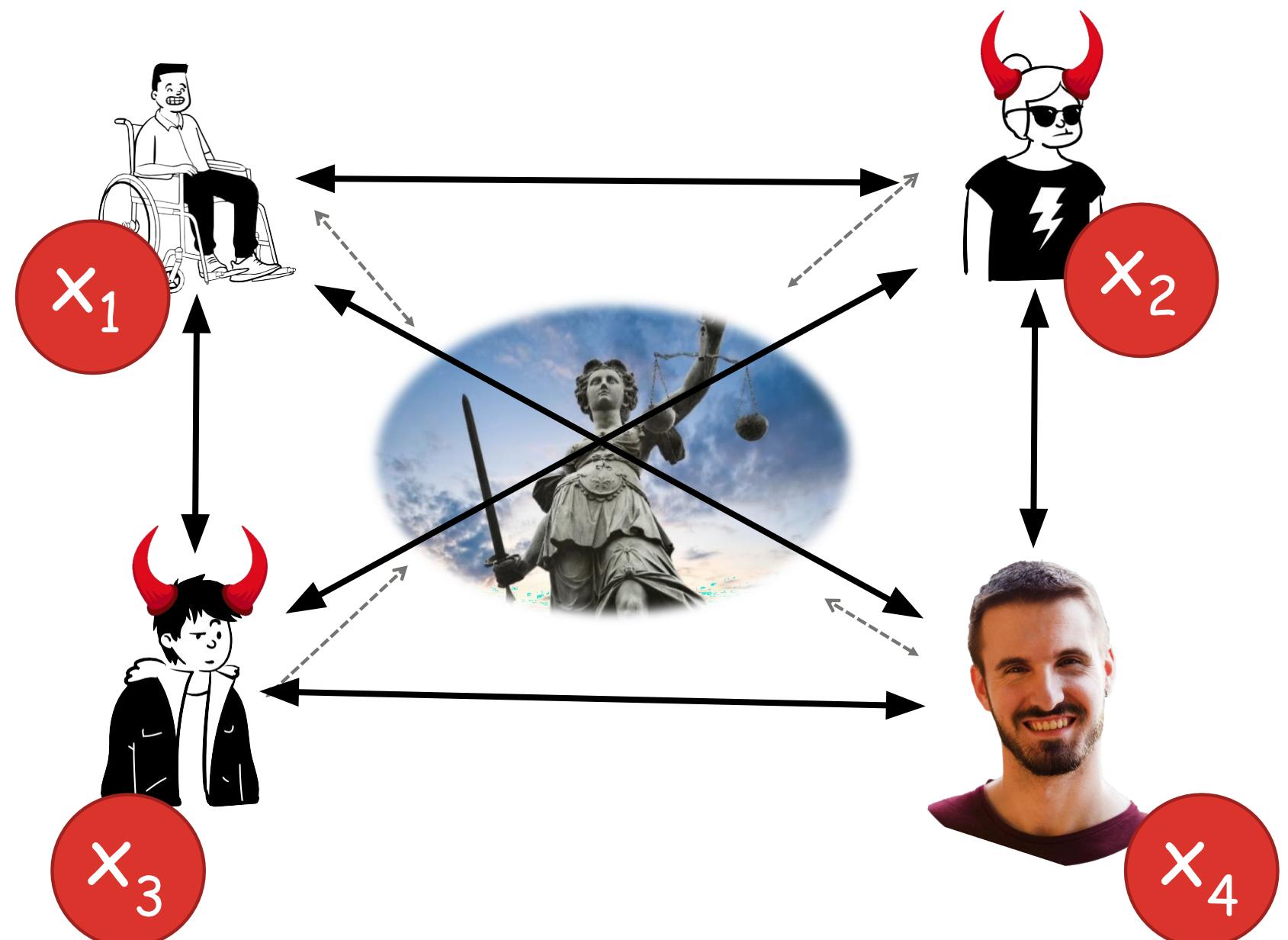
...

Problema con 3^a Parte Confianza:

Punto único de fallo.

Muchas veces, no existen.

II Multi-Party Computation: Intuición de seguridad



$$y = f(x_1, x_2, x_3, x_4)$$

Lo que vuelve difícil MPC es la presencia de un Adversario que participa en el protocolo y corrompe a ciertas entidades para coordinar su ataque.

- Corrupción pasiva: Las entidades corruptas hacen lo que deben, pero ponen información en conjunto para tratar de aprender más de la cuenta.
- Corrupción activa: Las entidades corruptas pueden actuar de forma arbitraria para sabotear los objetivos de seguridad.

Queremos lograr todas las propiedades que lograríamos con una tercera parte de confianza ¡sin ella!

¿Quién utiliza Multi-Party Computation?

Acronis



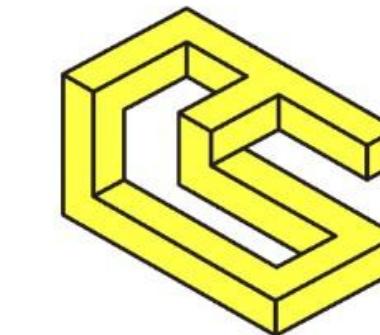
ARPA

atato



BOSCH

Cape Privacy



CUSTONOMY

CYBAVO

CYBERNETICA

DESILO



HEΛΛN CRYPTO LAB

Genreon



inpher

IJS TECHNOLOGIES



Magnite

Meta

Fuente: <https://www.mpcalliance.org/>

¿Quién utiliza Multi-Party Computation?

METACO

million

10th party

Palisade

PARFIN

Partisia

Partisia
Blockchain

PlatON

Portal

PROTEGO
TRUST BANK

Pyte.

qedit

Qredo

Roseman Labs

SAFEHERON

SAFEMATRIX

salesforce

SEPIOR
By BLOCKDAEMON

SILENCE
LABORATORIES

SPATIUM

TAURUS

TNO

TRAIL
OF BITS

TUNE INSIGHT

UNBOUND

verichains
CYBERSECURITY

XTENDR

Fuente: <https://www.mpcalliance.org/>

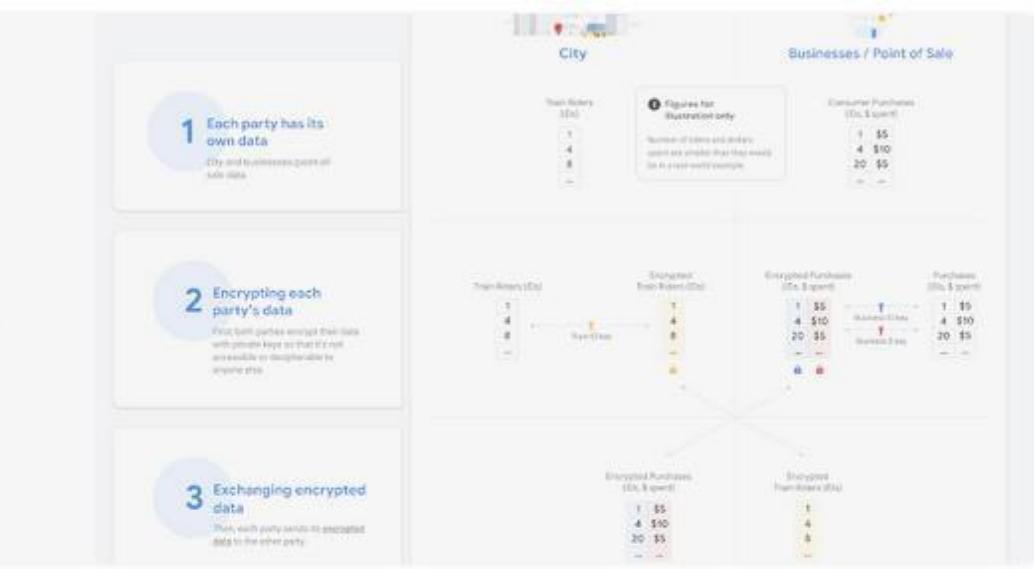
¿Quién utiliza Multi-Party Computation?



Google Private Join and Compute

Google's Private Join and Compute service is a new type of MPC that augments the core Private Set Intersection (PSI)...

Jun 27, 2023 · Infrastructure

A diagram illustrating the three steps of Google's Private Join and Compute service. Step 1: 'Each party has its own data' (City and businesses/grocery store data). Step 2: 'Encrypting each party's data' (Two bank parties encrypt their data with private keys so that it's not accessible or decipherable by anyone else). Step 3: 'Exchanging encrypted data' (Then, each party sends its encrypted data to the other party). To the right of the steps is a screenshot of a dashboard titled 'Businesses / Point of Sale' showing tables for 'Businesses' and 'Consumer Purchases'.

Divvi Up, A Privacy-Respecting System for Aggregate Statistics

Divvi Up is the Internet Security Research Group's system for private statistical aggregation of software telemetry. Divvi...

Jun 27, 2023 · Private Analytics

The logo for Divvi Up consists of the word 'Divvi' in a blue, lowercase, sans-serif font followed by 'Up' in a larger, bold, blue, sans-serif font. Below the logo, the tagline 'Data divided. Data secured.' is written in a smaller, blue, sans-serif font.

| Multi-Party Computation: ¿A partir de qué primitivas?

Garbled Circuits (Circuitos Cifrados)

Compartición de Secretos (Secret Sharing)

Oblivious Transfer (Transferencia Inconsciente)

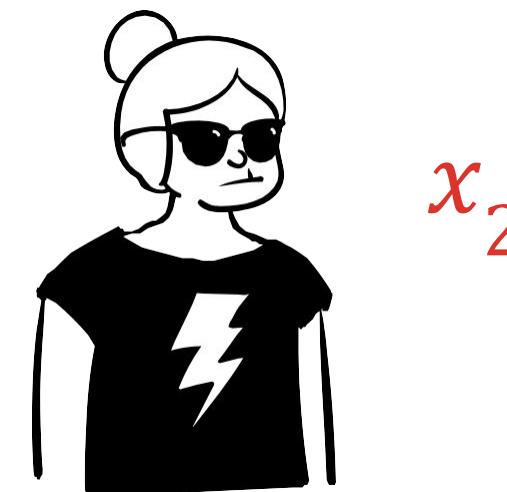
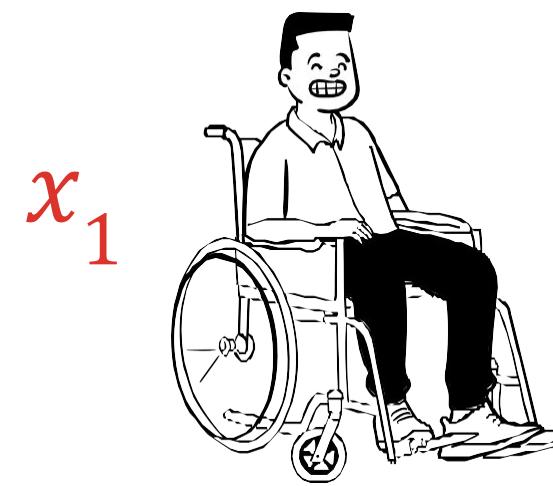
Cifrado homomórfico (Homomorphic Encryption)

...

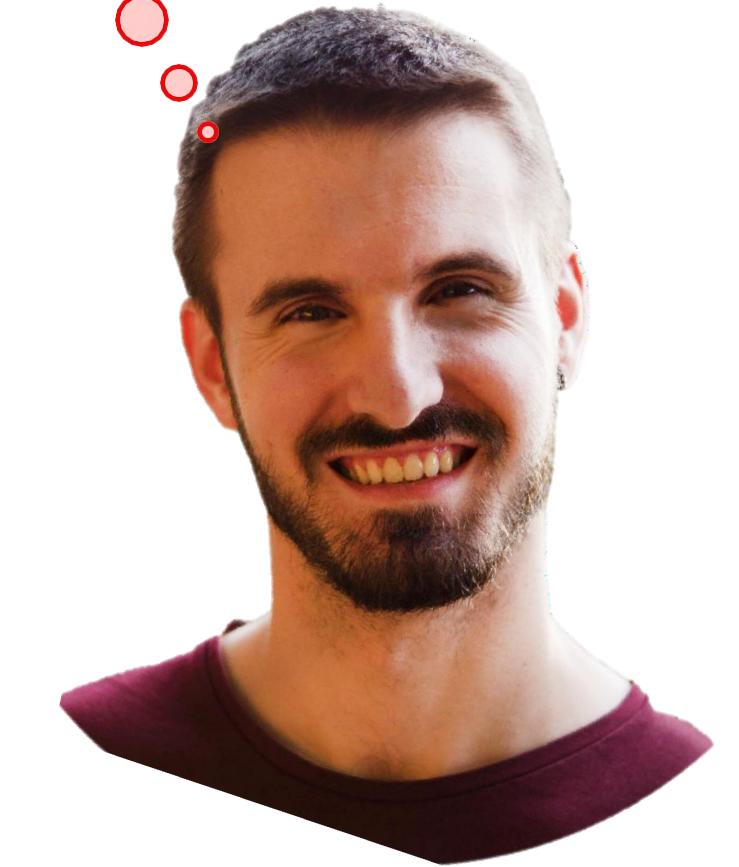


Bloque 1: Repartición de secretos (mediante esquemas lineales)

I ¿Cuánta gente copia?



¿Cuántos estudiantes
copian en el examen?



$$f(x_1, x_2, x_3) = x_1 + x_2 +$$

x_3



- Una función muy sencilla (lineal).
- La vamos a calcular utilizando exclusivamente compartición de secretos, una de las herramientas básicas de Multi-Party Computation.

I Compartición de secretos: Definición

Definition: Compartición de secretos

Sea \mathbb{F} un cuerpo finito y sean $n, t \in \mathbb{Z}$ tales que $0 \leq t < n$. Sean las entidades P_1, P_2, \dots, P_n y un *Compartidor* en posesión de un secreto $s \in \mathbb{F}$. Un esquema (n, t) -umbral de compartición de secretos consta de las dos siguientes fases:

1. **Fase de compartición:** El *Compartidor* “fragmenta” s en n partes, $s_1, s_2, \dots, s_n \in \mathbb{F}$ y la entidad P_i recibe su parte $s_i \in \mathbb{F}$.
2. **Fase de reconstrucción:** Al menos $t + 1$ entidades envían su parte a quien quieran que reconstruya s .

Y satisface las siguientes propiedades:

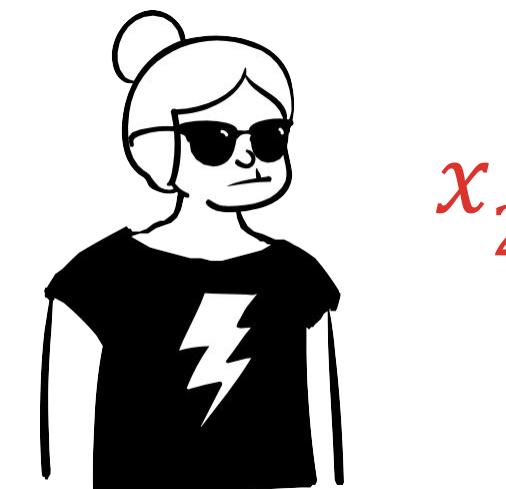
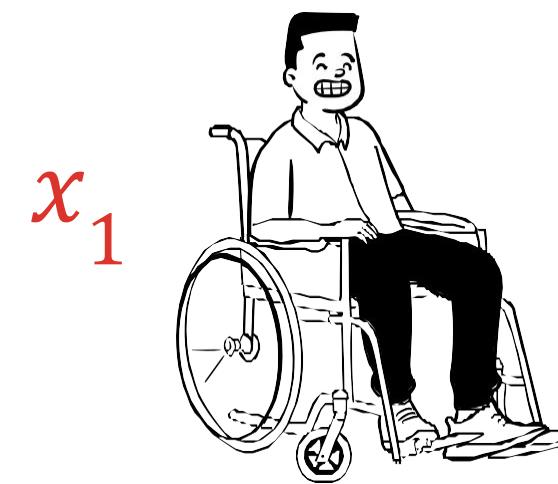
- **t -privacidad:** Cualquier conjunto de t sumo partes no revela *niguna información* sobre el secreto $s \in \mathbb{F}$.
- **$(t + 1)$ -reconstrucción:** Cualquier conjunto de $t + 1$ partes determina de forma única el secreto $s \in \mathbb{F}$.

Decimos que el esquema es *lineal* si además satisface que $\forall s, t \in \mathbb{F}$ compartidos como $(s_1, s_2, \dots, s_n) \in \mathbb{F}^n$ y $(t_1, t_2, \dots, t_n) \in \mathbb{F}^n$, tenemos que $(s_1 + t_1, s_2 + t_2, \dots, s_n + t_n)$ es una compartición de $s + t \in \mathbb{F}$.

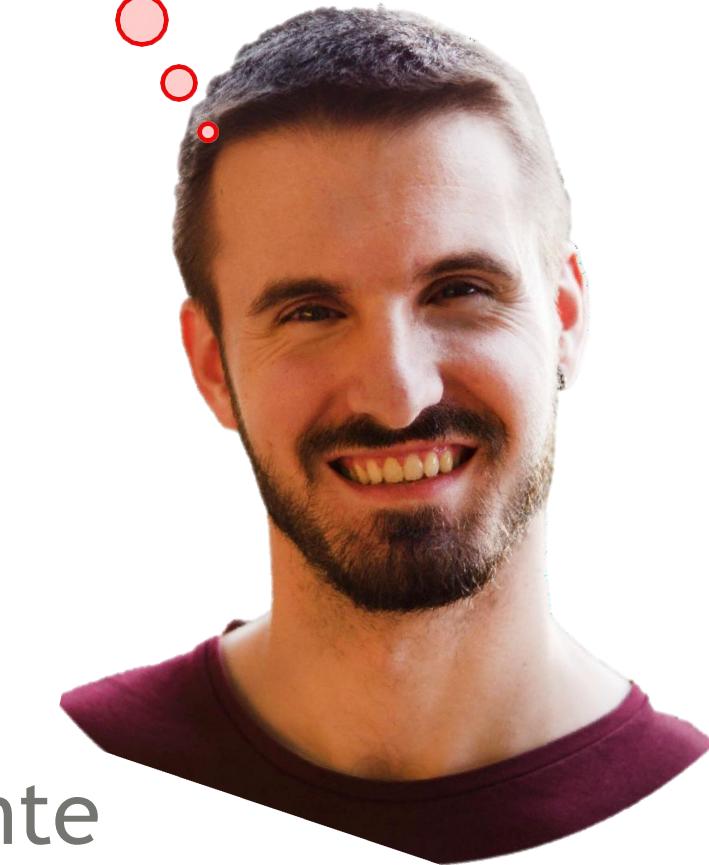
Abusaremos notación, y nos restringiremos a esquemas de compartición de secretos que sean sobre un cuerpo finito \mathbb{F} , umbrales y lineales (sobre \mathbb{F}).

Utilizaremos $[s]$ para referirnos al secreto junto con sus fragmentos $[s] = (s; s_1, s_2, \dots, s_n)$.

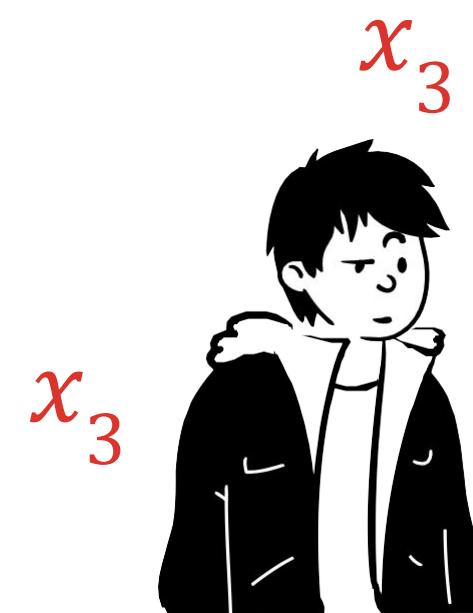
I ¿Cuánta gente copia?



¿Cuántos estudiantes copian en el examen?



$$f(x_1, x_2, x_3) = x_1 + x_2 +$$



- Paso 1: Utilizando un esquema lineal, cada estudiante P_i comparte su secreto entre todos: $[x_i]$
- Paso 2: Los estudiantes suman sus partes de cada secreto para calcular conjuntamente

$$[x_1 + x_2 + x_3] = [x_1] + [x_2] + [x_3]$$

- Paso 3: Reconstruimos el secreto $[x_1 + x_2 + x_3]$.

Compartición de secretos aditiva



ADDITIVE SECRET SHARING



I Compartición de secretos aditiva

Sea $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$; $\mathbb{Z}/p\mathbb{Z} = (0, 1, \dots, p-1)$, p es un número primo.

1. Fase de compartición:

I. *Compartidor* escoge de forma unif. aleatoria $s_1, s_2, \dots, s_n \in \mathbb{F}_p$ tales que $s_1 + s_2 + \dots + s_n = s$.

P.ej: Elige $s_1, s_2, \dots, s_{n-1} \in \mathbb{F}_p$ de forma uniformemente aleatoria.

Define $s_n = s - (s_1 + s_2 + \dots + s_{n-1})$.

II. *Compartidor* envía la parte s_i a P_i .



1. Fase de reconstrucción:

a. Cada P_i envía s_i a la entidad que quieren que reconstruya el secreto.

b. Dicha entidad calcula $s = s_1 + s_2 + \dots + s_n$.



¿Cuál es el umbral t ? ¿Por qué es t -privado y $(t+1)$ -reconstruible?

|| Pros/cons de la compartición de secretos aditiva

VENTAJAS

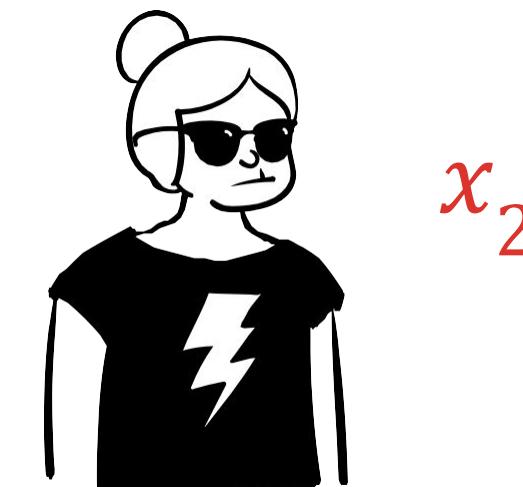
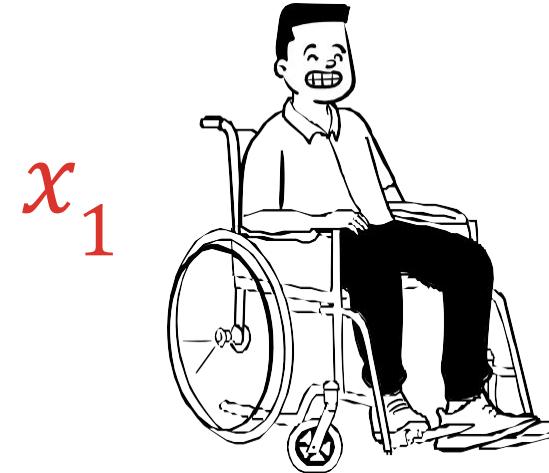
- Tamaño óptimo de las partes (cada parte “es tan grande” como el secreto).
- Muy eficiente a nivel computacional.

INCONVENIENTES

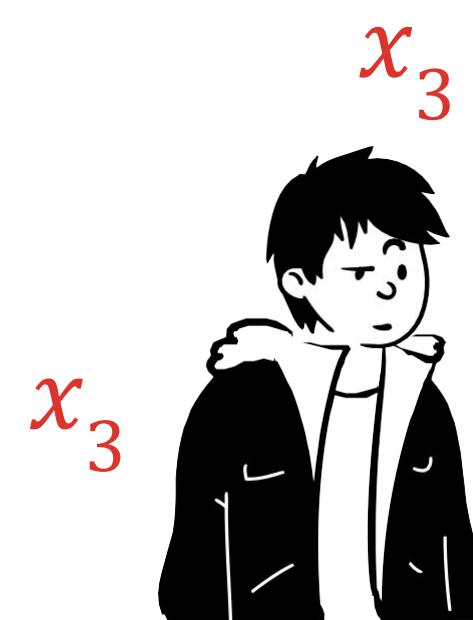
- El umbral siempre es $t = n - 1$.
- Aunque es lineal, no tiene propiedades multiplicativas (segunda parte de esta charla).
- Por sí mismo, no ofrece ningún tipo de resistencia ante adversarios activos.



Resolvamos paso a paso el problema de cuanta gente copia utilizando compartición de secretos aditiva



¿Cuántos estudiantes copian en el examen?



$$f(x_1, x_2, x_3) = x_1 + x_2 +$$

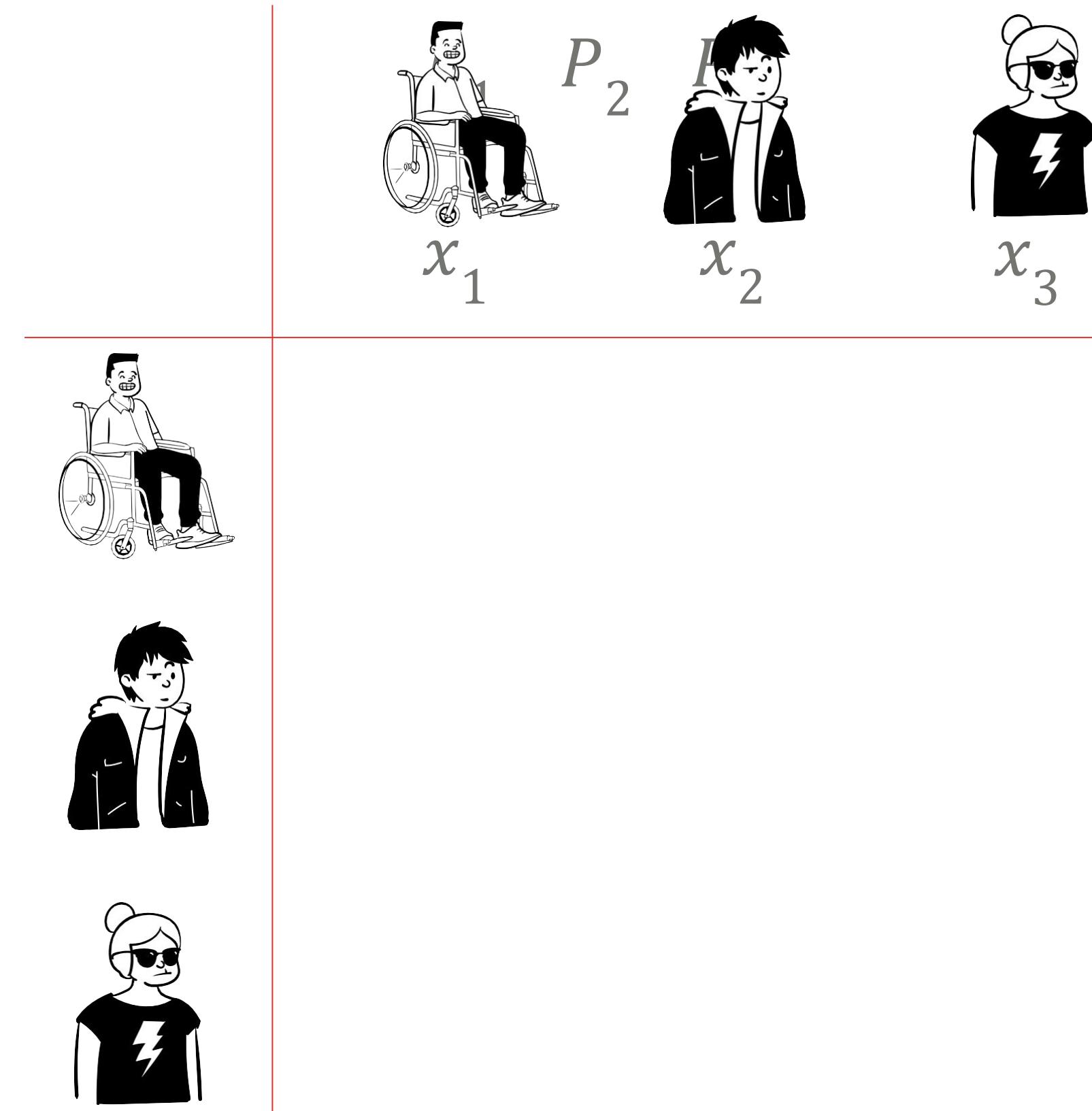
x_3

- Paso 1: Utilizando un esquema lineal, cada estudiante P_i comparte su secreto entre todos: $[x_i]$
- Paso 2: Los estudiantes suman sus partes de cada secreto para calcular conjuntamente

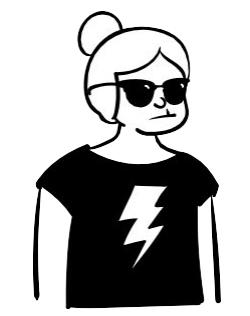
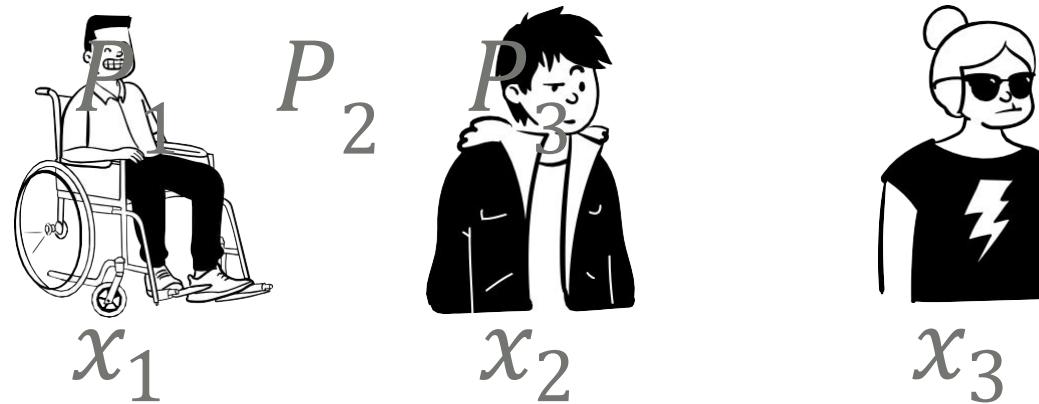
$$[x_1 + x_2 + x_3] = [x_1] + [x_2] + [x_3]$$

- Paso 3: Reconstruimos el secreto $[x_1 + x_2 + x_3]$.

Compartición de secretos aditiva: Suma



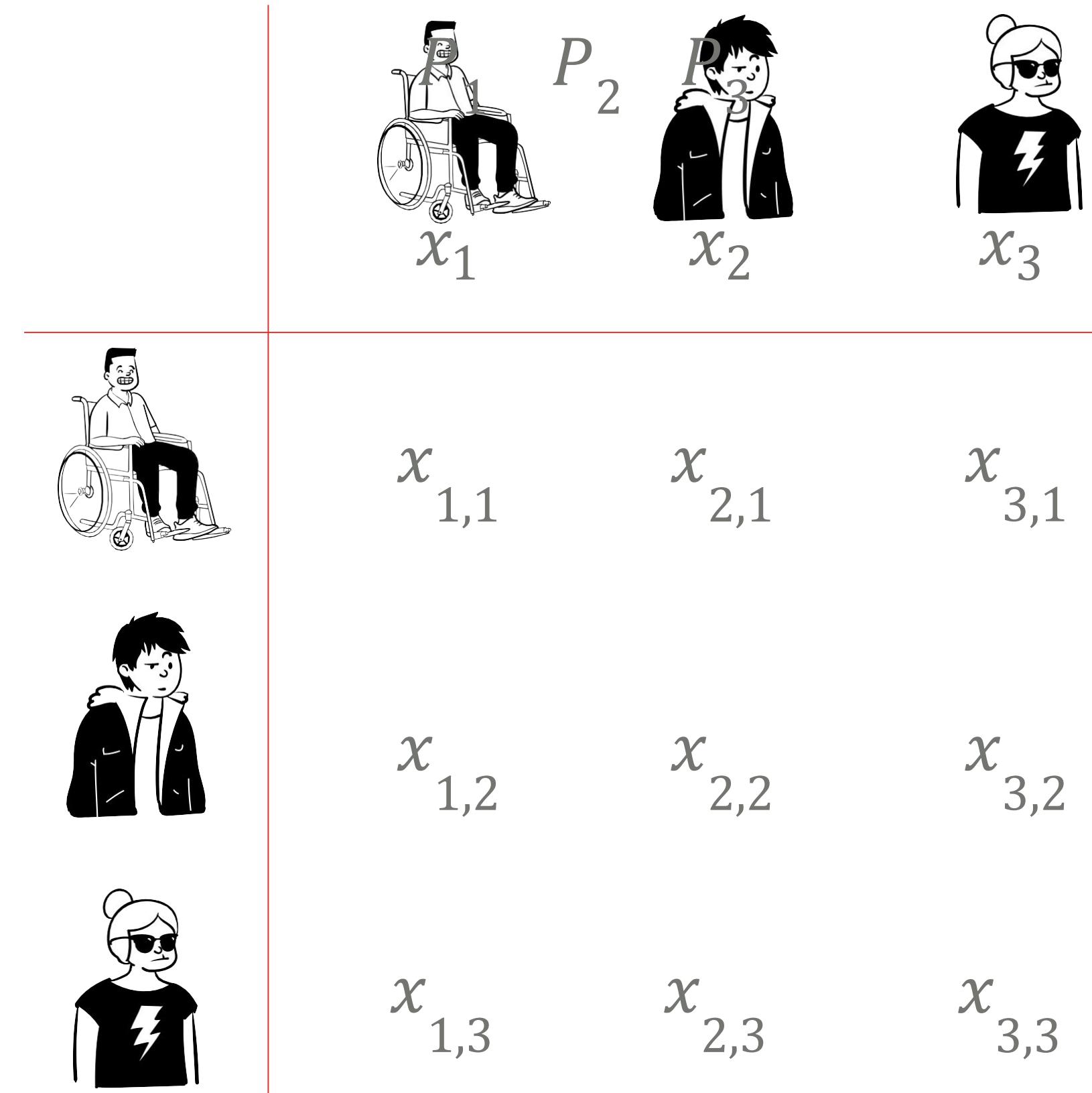
Compartición de secretos aditiva: Suma



Fase de compartición:
Cada entidad comparte su
secreto

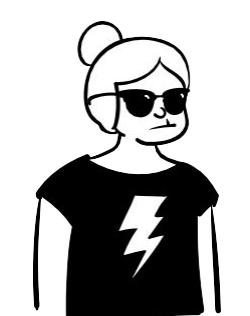
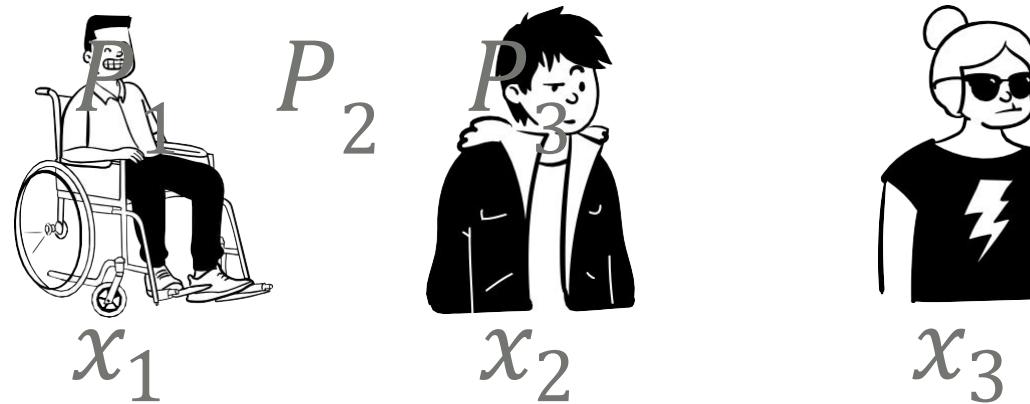
El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

Compartición de secretos aditiva: Suma



El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

Compartición de secretos aditiva: Suma

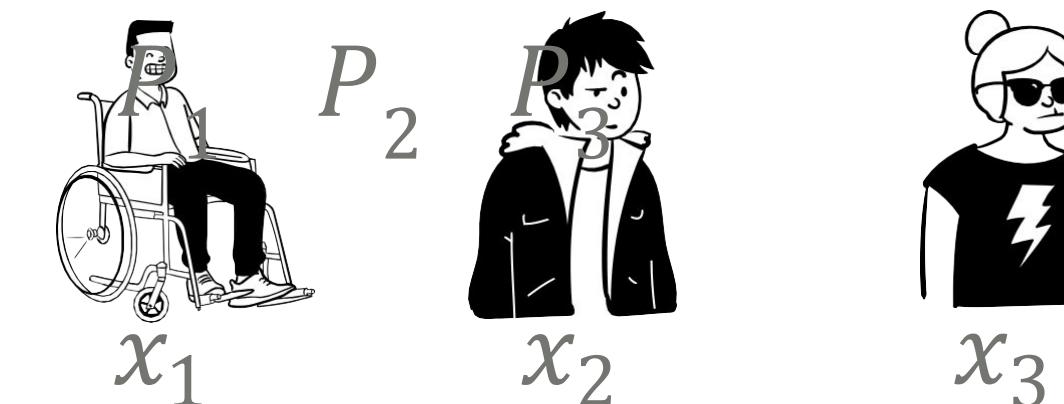


Fase de cálculo:

Cada entidad suma las partes de los secretos que ha recibido

El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

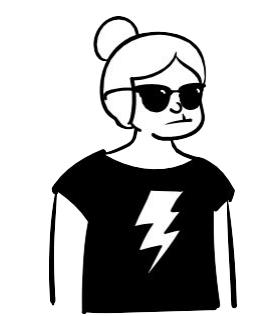
Compartición de secretos aditiva: Suma



$$x_{1,1} + x_{2,1} + x_{3,1} =: s_1$$



$$x_{1,2} + x_{2,2} + x_{3,2} =: s_2$$



$$x_{1,3} + x_{2,3} + x_{3,3} =: s_3$$

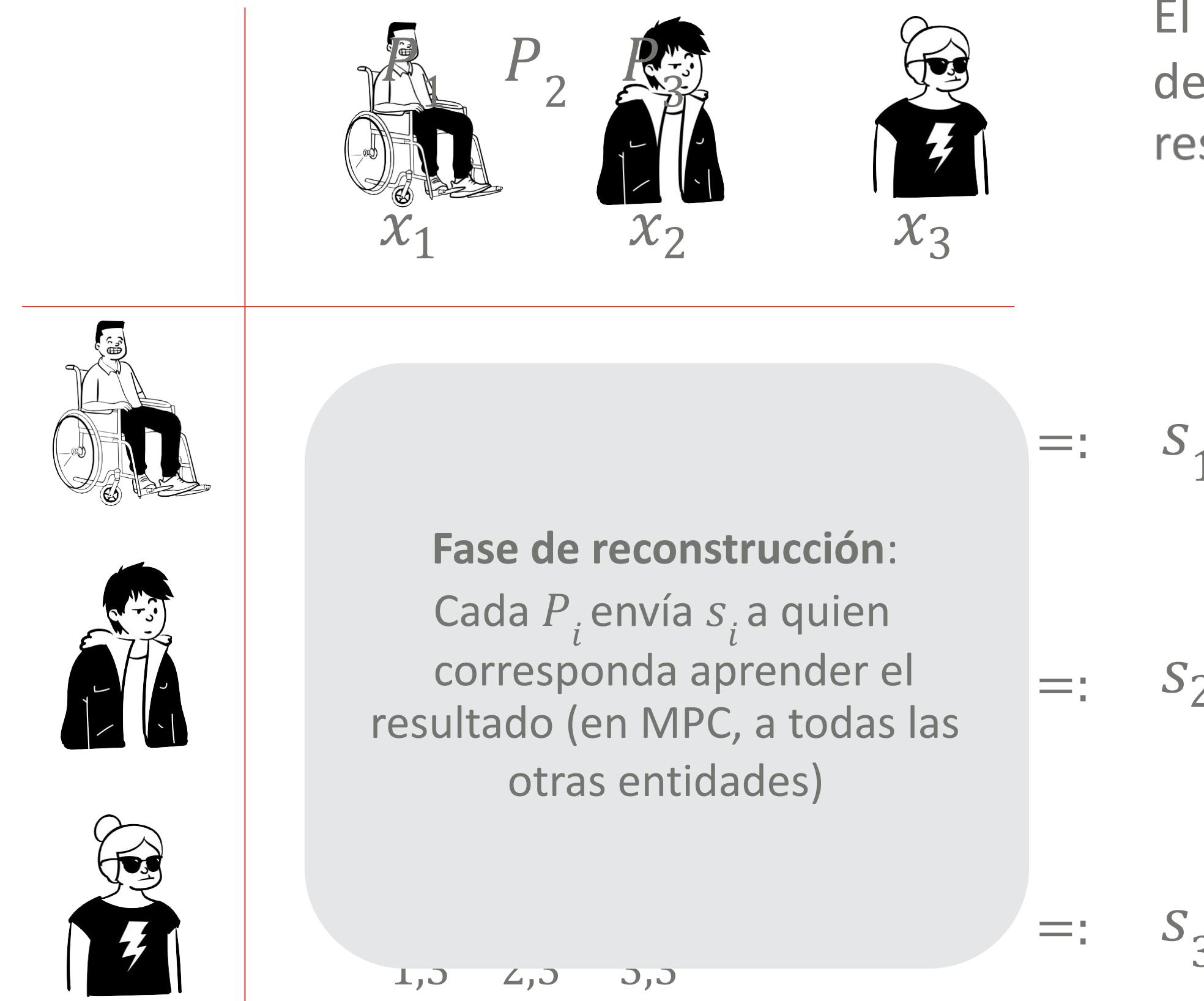
El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

Idea Fundamental:

(s_1, s_2, s_3) es una compartición de secretos aditiva de $x_1 + x_2 + x_3$.

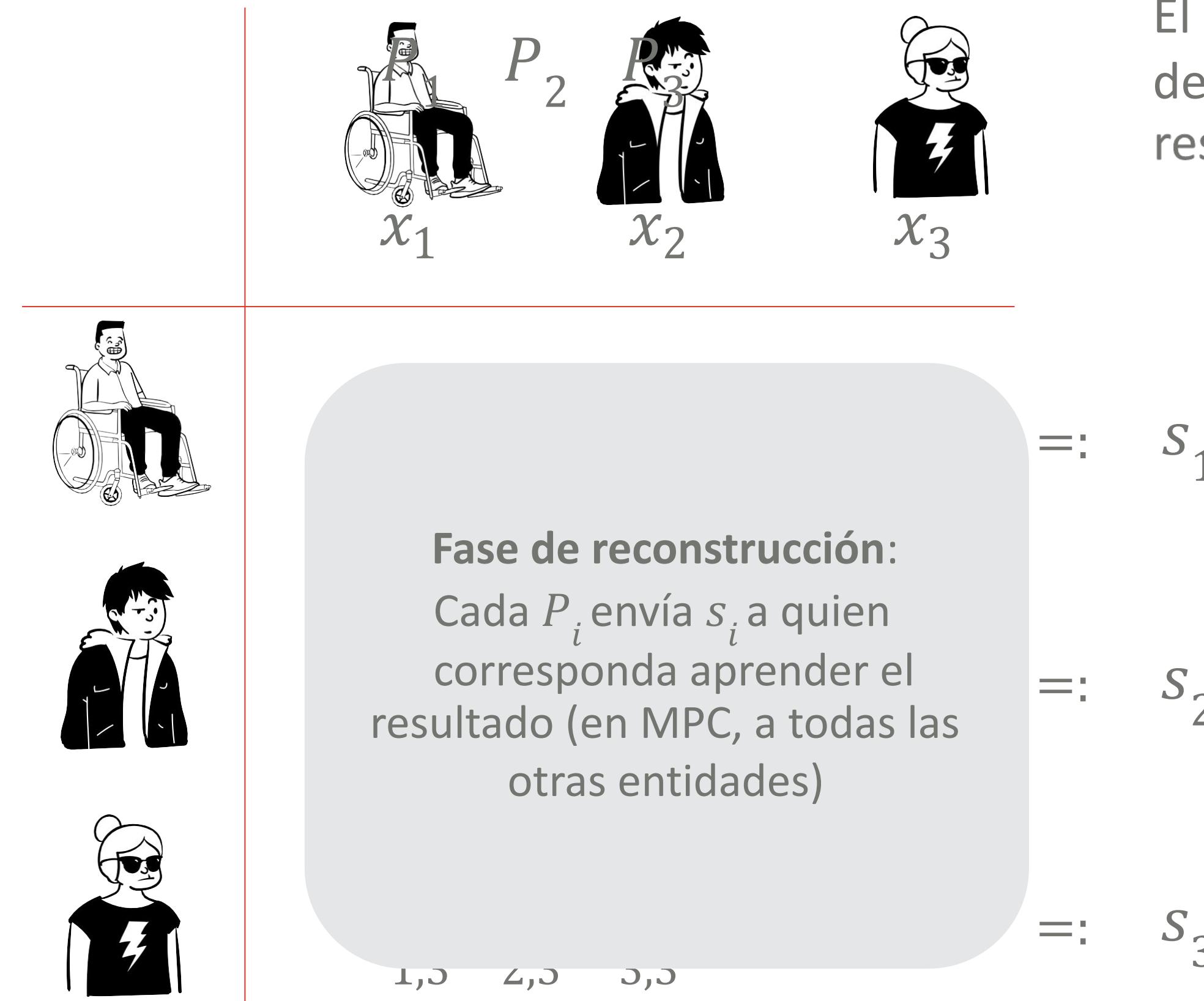
$$\begin{aligned} s_1 +_2 s_3 + s &= \sum_{j=1}^3 x_{i,j} \\ x_1 + x_2 + x_3 &= \end{aligned}$$

Compartición de secretos aditiva: Suma



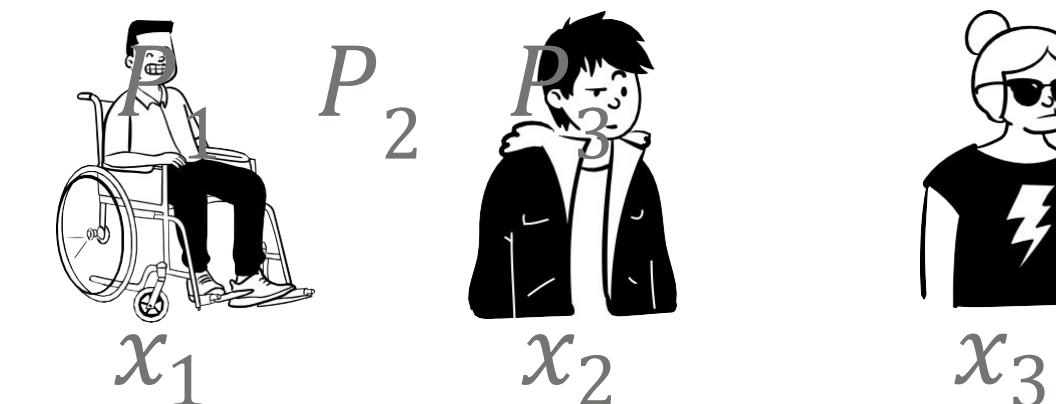
El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

Compartición de secretos aditiva: Suma



El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

Compartición de secretos aditiva: Suma



El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.



$$x_{1,1} + x_{2,1} + x_{3,1} =: s_1$$



$$x_{1,2} + x_{2,2} + x_{3,2} =: s_2$$

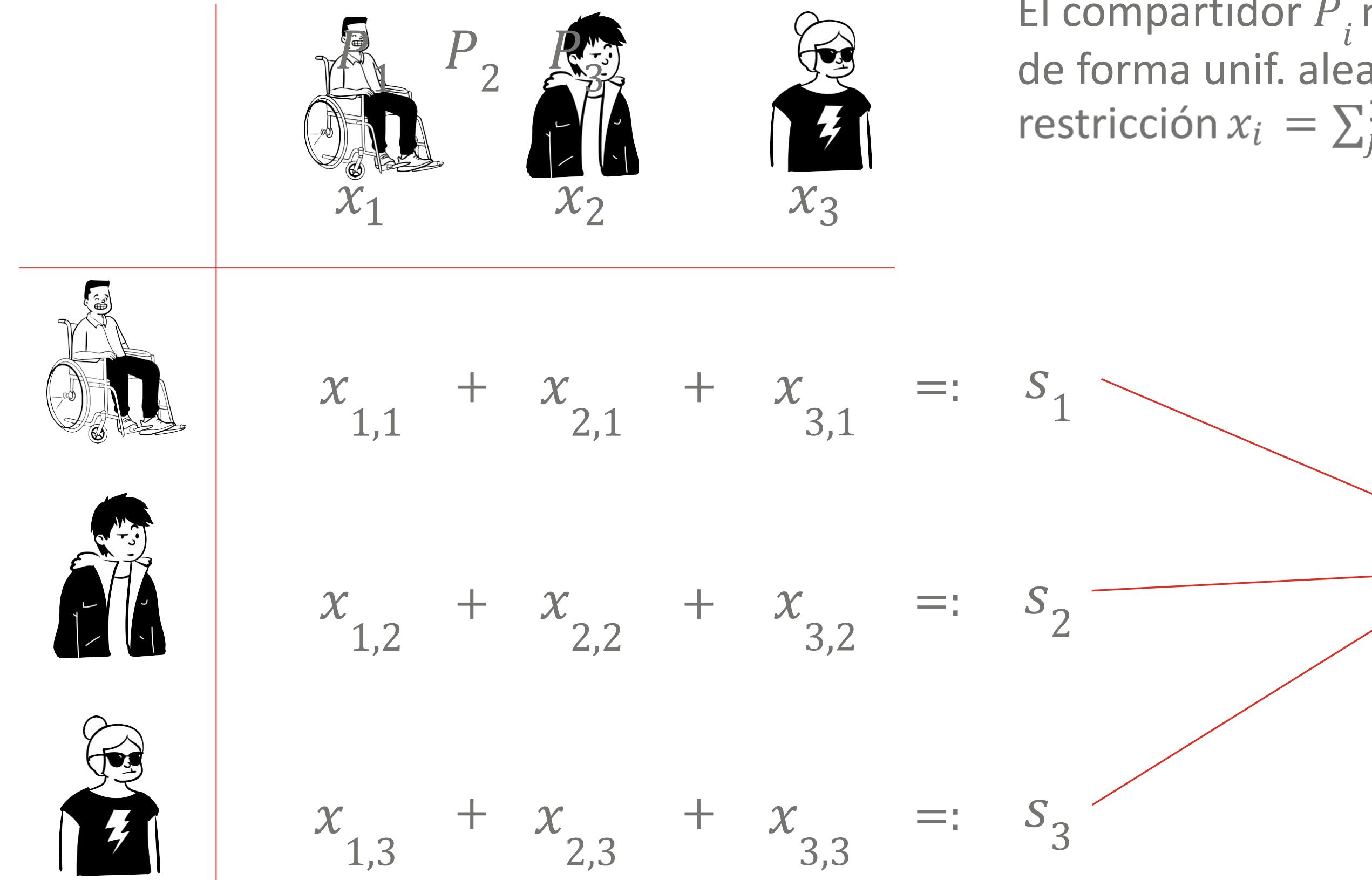


$$x_{1,3} + x_{2,3} + x_{3,3} =: s_3$$



$$s_1 + s_2 + s_3 = \\ x_1 + x_2 + x_3$$

Compartición de secretos aditiva: Suma



El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

Compartición de secretos replicada



REPLICATED S RET SHARING



Compartición de secretos replicada (con 3 entidades)

Sea $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$; $\mathbb{Z}/p\mathbb{Z} = (0, 1, \dots, p - 1)$, p es un número primo.

1. Fase de compartición:

- I. *Compartidor* escoge de forma unif. aleatoria $s_1, s_2, s_3 \in \mathbb{F}_p$ tales que $s_1 + s_2 + s_3 = s$.

P.ej: Elige $s_1, s_2, \in \mathbb{F}_p$ de forma uniformemente aleatoria.

Define $s_3 = s - (s_1 + s_2)$.

- II. *Compartidor* envía las partes s_{i-1} y s_{i+1} a P_i .

1. Fase de reconstrucción:

- a. Cada P_i envía s_{i-1} y s_{i+1} a la entidad que quieren que reconstruya el secreto.
- b. Dicha entidad calcula $s = s_1 + s_2 + s_3$.



Cuál es el umbral t ? ¿Por qué es t -privado y $(t+1)$ -reconstruible? ¿Es lineal?

|| Pros/Cons de la compartición de secretos replicada

VENTAJAS

- Tiene propiedades multiplicativas (lo veremos en la última clase).
- Ante un adversario pasivo, la reconstrucción puede requerir de menos comunicación que la compartición de secretos aditiva (siguientes diapositivas).
- Tiene propiedades de detección de errores. Ante un Adversario activo, se puede detectar si una entidad se desvía del protocolo (siguientes diapositivas).

INCONVENIENTES

- El tamaño de las partes es superior al tamaño del secreto (el doble de grande para t=1, n=3).
- Aunque se puede generalizar a otros valores de (n, t), el tamaño de las partes del secreto crece rapidísimo ($\binom{n}{t}$ elementos de \mathbb{F}_p por entidad).

I ¿Cuánta gente copia? Versión replicada



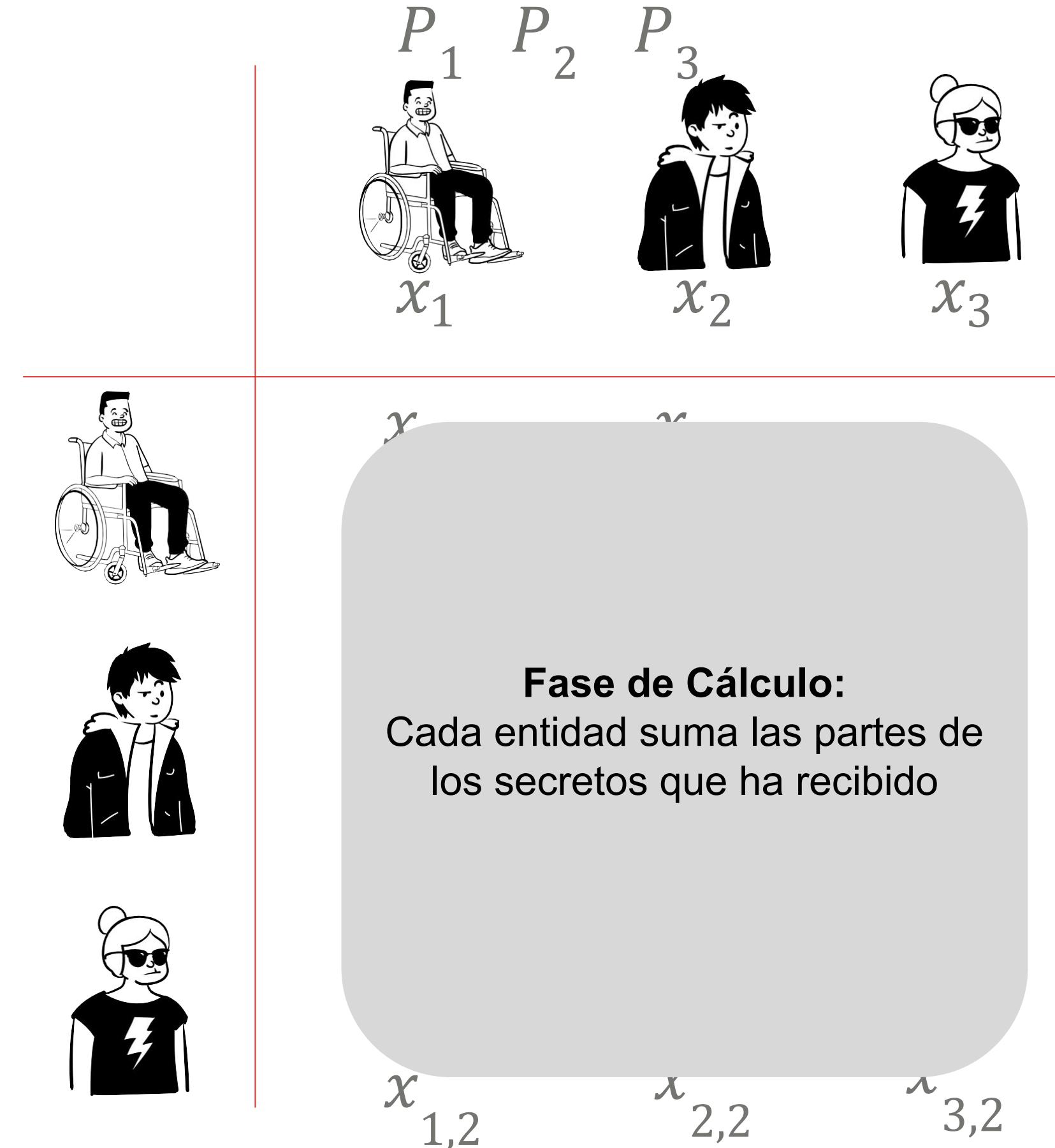
El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

I Compartición de secretos replicada: Suma

	P_1	P_2	P_3
x_1			
$x_{1,2}$		$x_{2,2}$	$x_{3,2}$
$x_{1,3}$		$x_{2,3}$	$x_{3,3}$
$x_{1,1}$	$x_{2,1}$	$x_{3,1}$	
$x_{1,3}$	$x_{2,3}$	$x_{3,3}$	
$x_{1,1}$	$x_{2,1}$	$x_{3,1}$	
$x_{1,2}$	$x_{2,2}$	$x_{3,2}$	

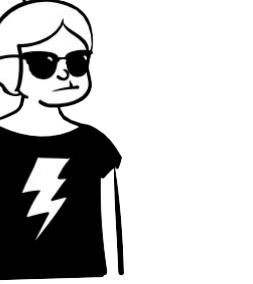
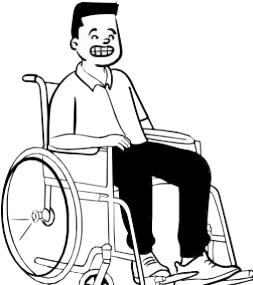
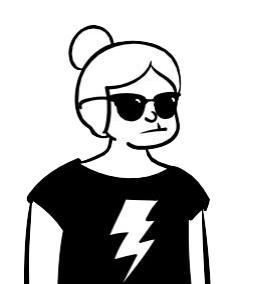
El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

I Compartición de secretos replicada: Suma



El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

I Compartición de secretos replicada: Suma

P_1	P_2	P_3	
			
x_1	x_2	x_3	
			s_2
	$x_{1,2} + x_{2,2} + x_{3,2} =:$		
	$+ x_{1,3} + x_{2,3} + x_{3,3} =:$		s_3
	$x_{1,1} + x_{2,1} + x_{3,1} =:$		s_1
	$x_{1,3} + x_{2,3} + x_{3,1} =:$		s_3
	$x_{1,1} + x_{2,1} + x_{3,1} =:$		s_1
	$x_{1,2} + x_{2,2} + x_{3,2} =:$		s_2

El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

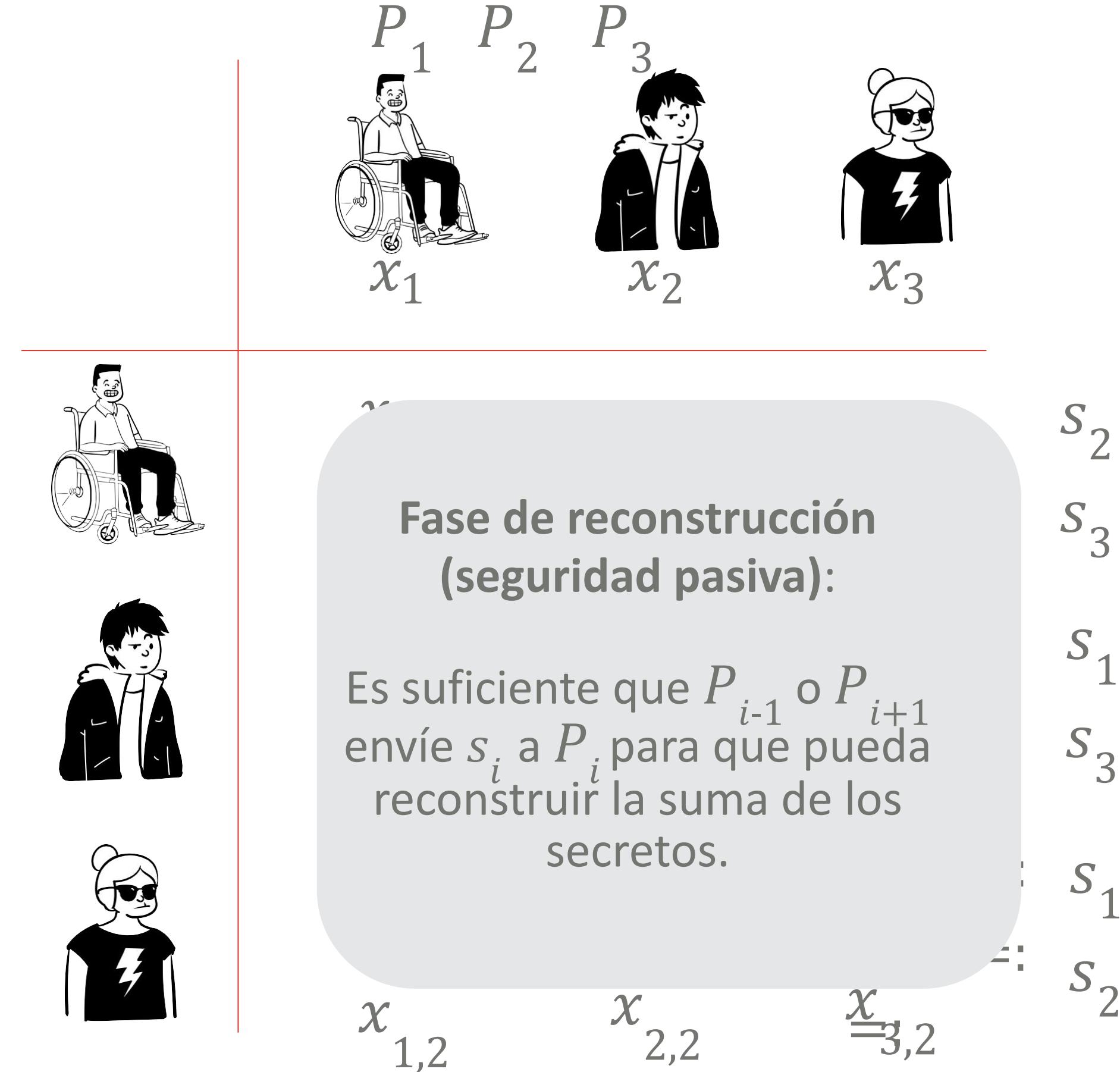
Idea Fundamental:

$((s_2, s_3), (s_1, s_3), (s_1, s_2))$ es una
compartición de secretos replicada
de $x_1 + x_2 + x_3$.

$$s_1 + s_2 + s_3 = \sum_{i,j=1}^3 x_{i,j}$$

$$x_1 + x_2 + x_3 =$$

I Compartición de secretos replicada: Suma



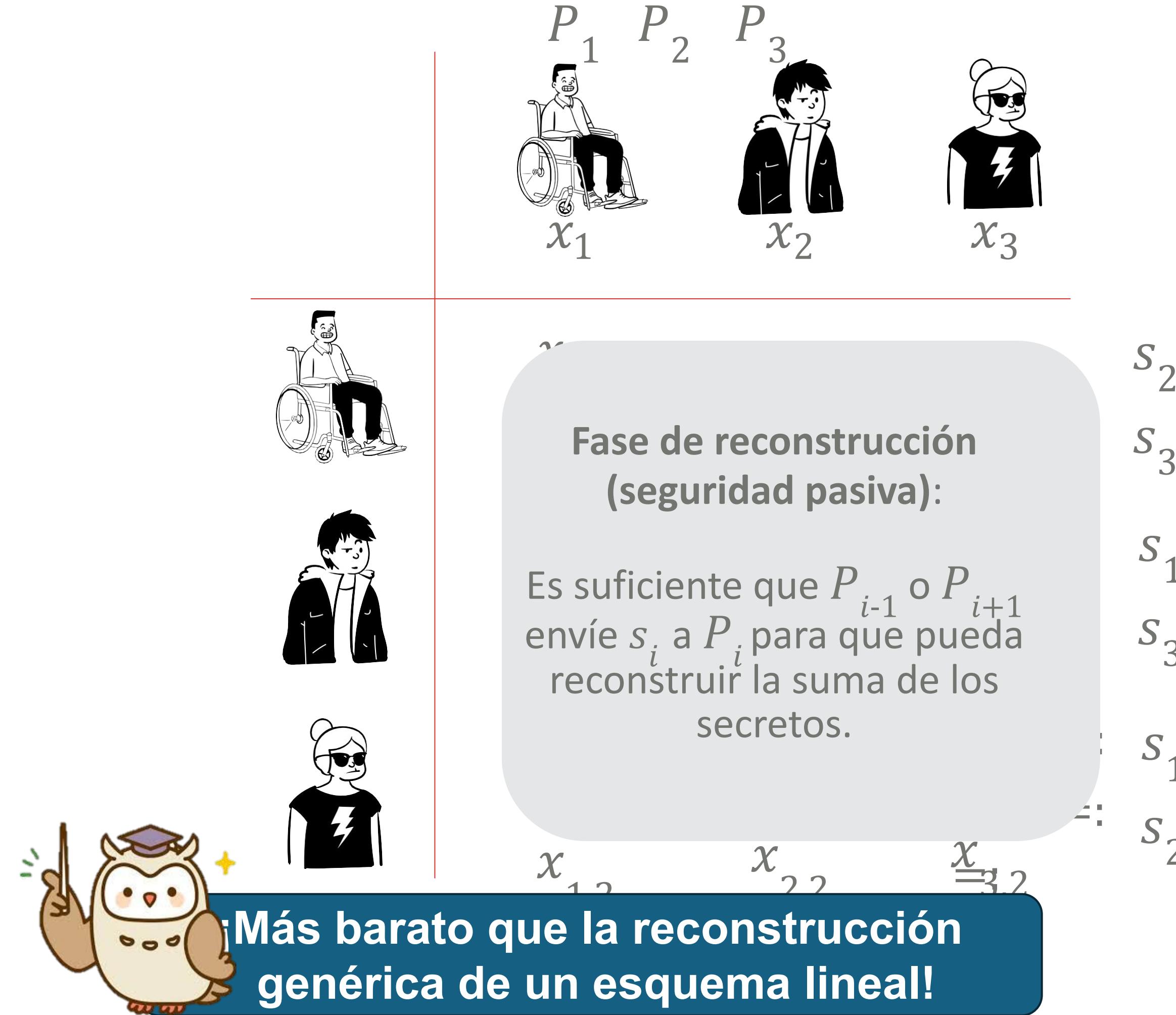
El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

Idea Fundamental:

$((s_2, s_3), (s_1, s_3), (s_1, s_2))$ es una
compartición de secretos replicada
de $x_1 + x_2 + x_3$.

$$s_1 + s_3 + s_2 = \sum_{j=1}^3 x_{i,j}$$
$$x_1 + x_2 + x_3 =$$

I Compartición de secretos replicada: Suma



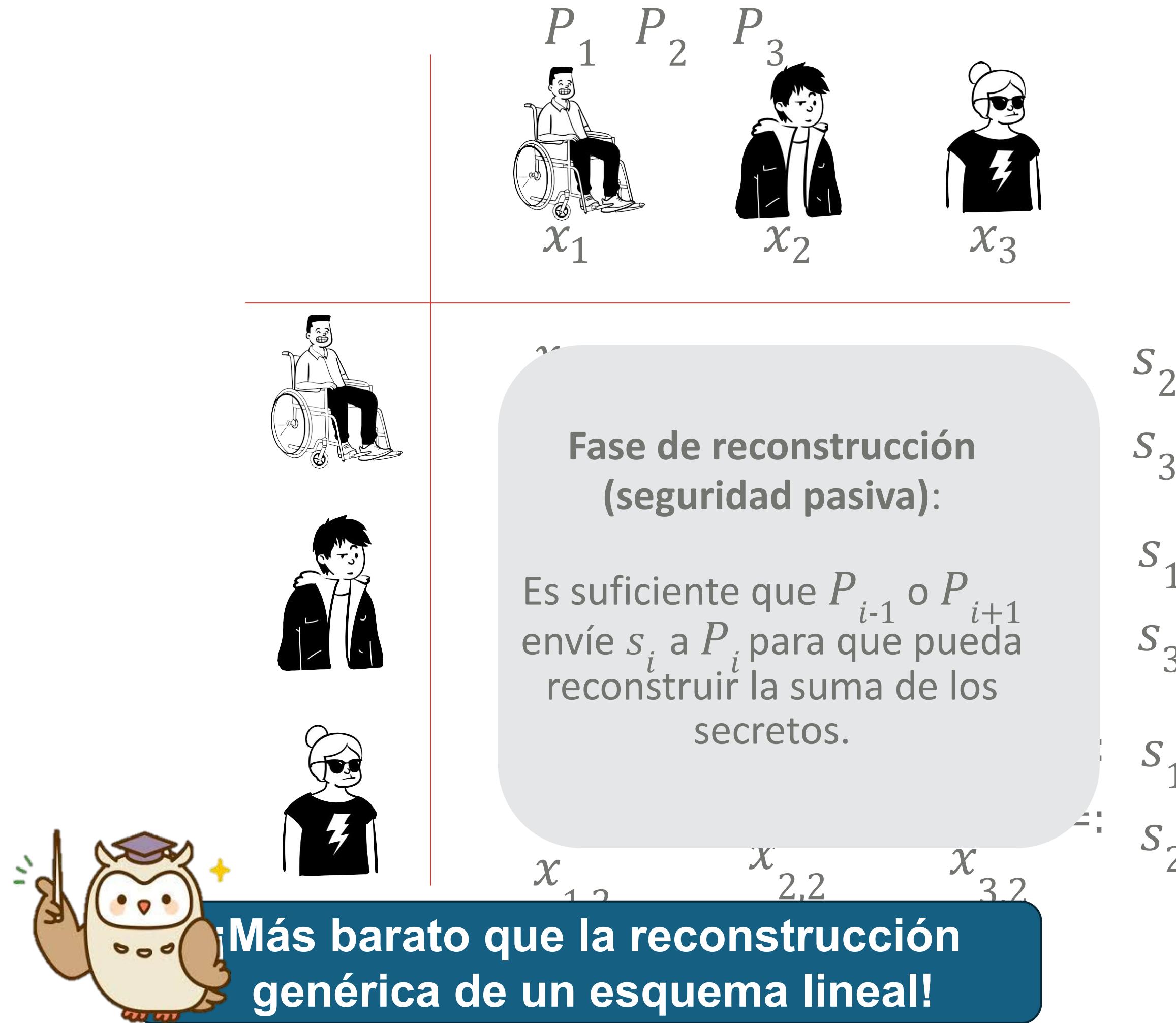
El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

s_2
 s_3
 s_1
 s_3
 s_1
 s_2
 s_2

Idea Fundamental:
((s_2, s_3), (s_1, s_3), (s_1, s_2)) es una
compartición de secretos replicada
de $x_1 + x_2 + x_3$.

$$s_1 +_2 s_3 + s_1 = \sum_{j=1}^3 x_{i,j} \\ x_1 + x_2 + x_3 =$$

I Compartición de secretos replicada: Suma

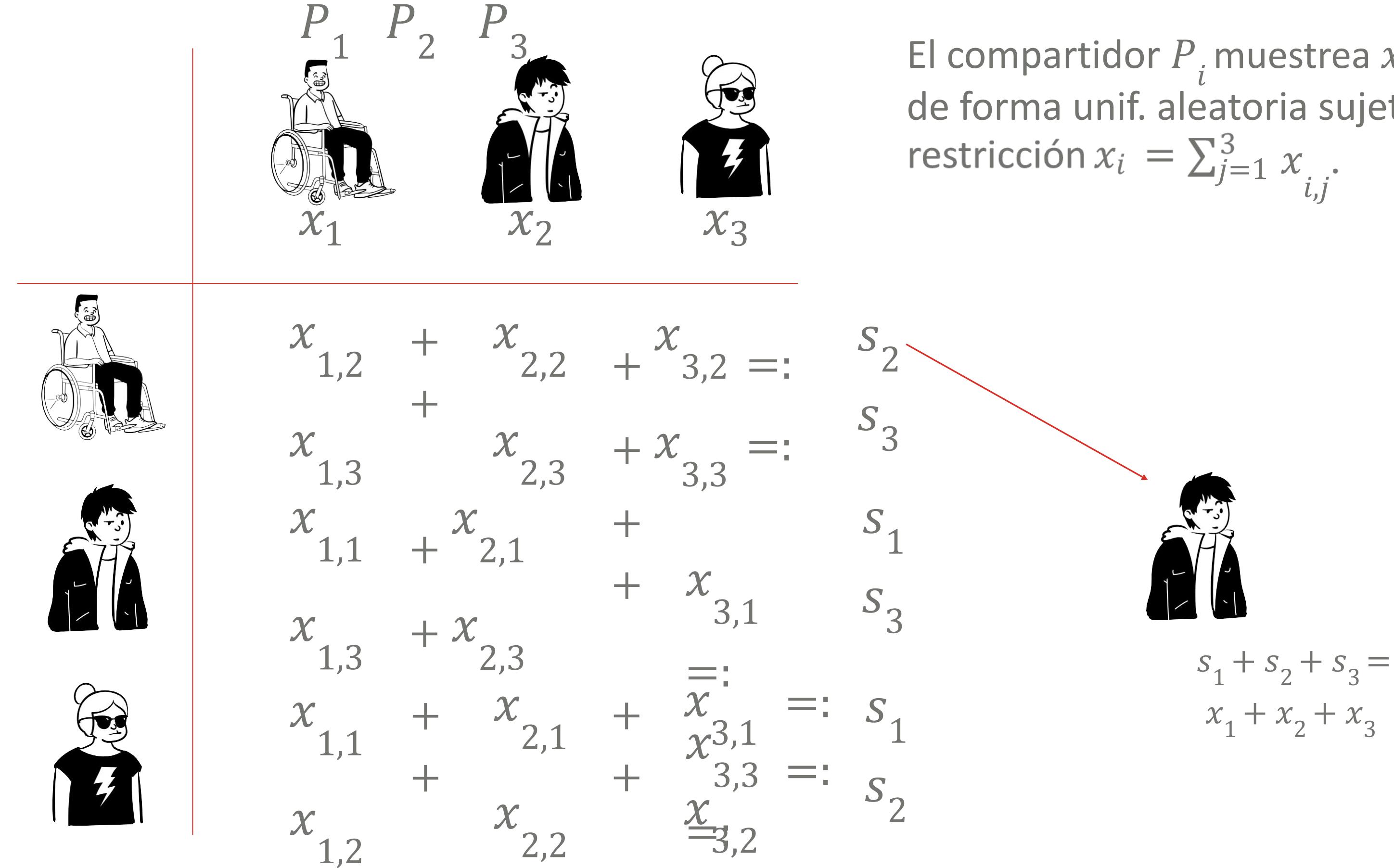


El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

S_2
 S_3
 S_1
 S_3
 S_1
 S_2

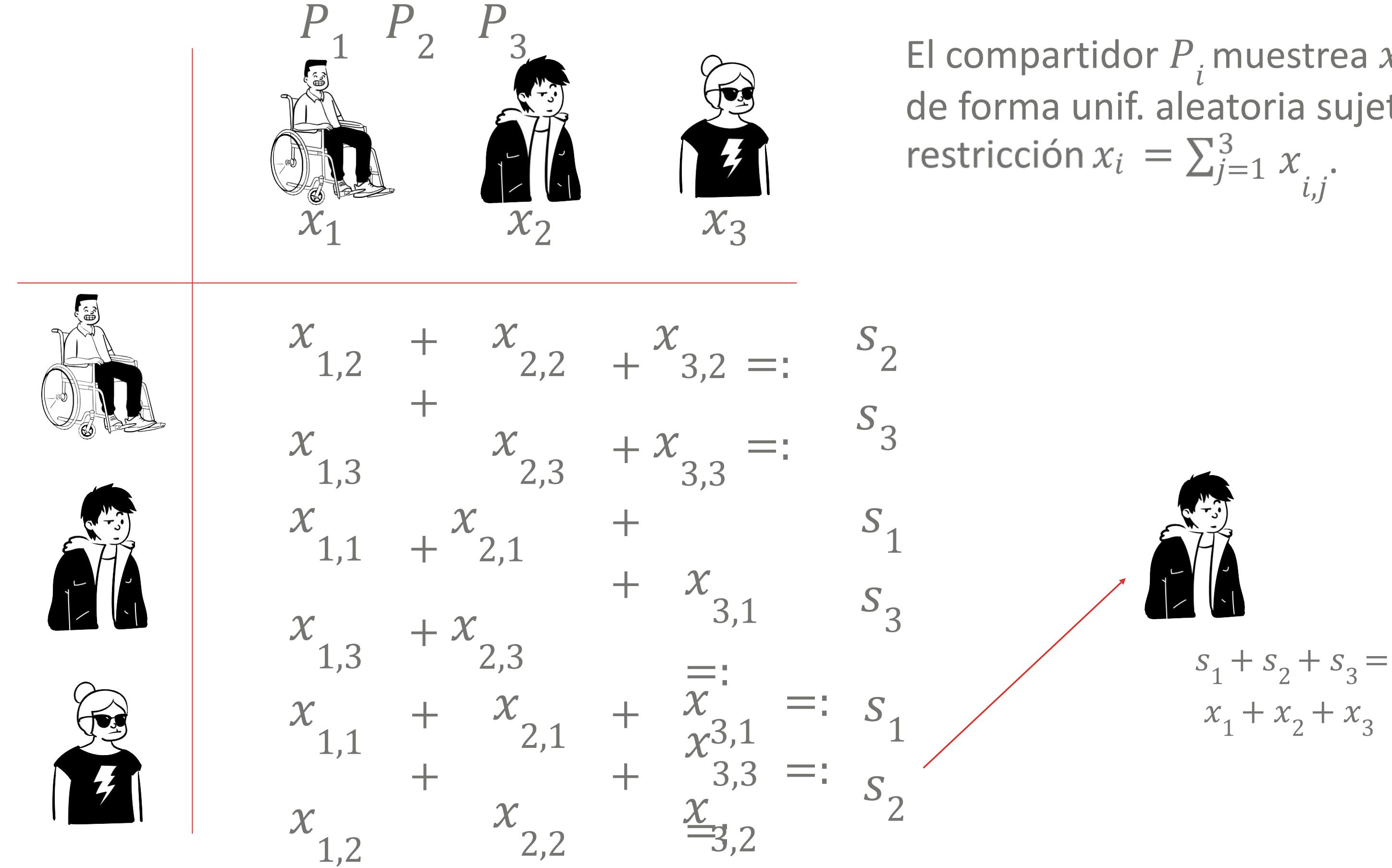


I Compartición de secretos replicada: Suma



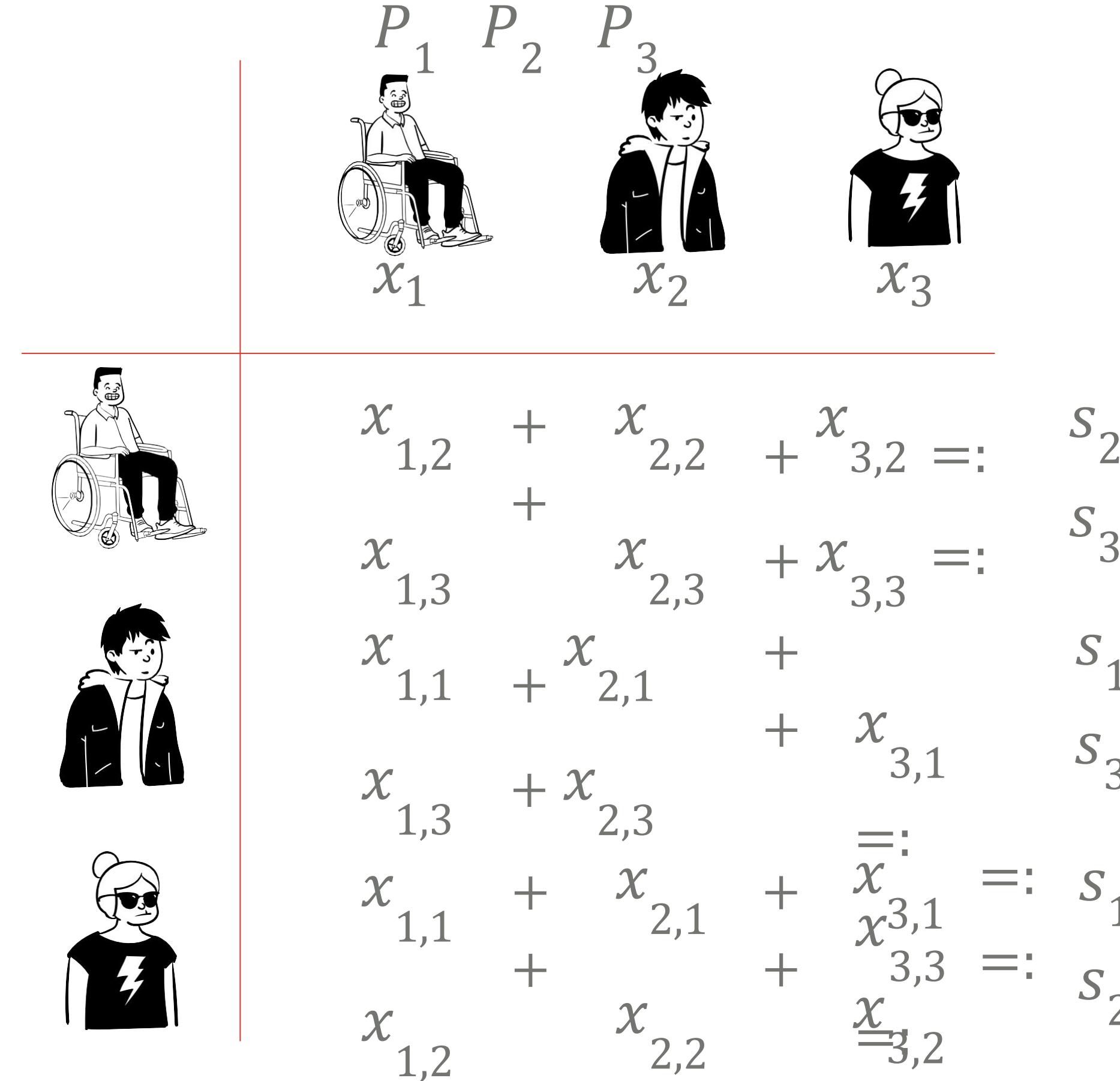
El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

I Compartición de secretos replicada: Suma

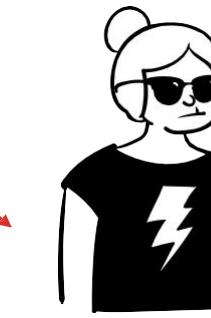


El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

I Compartición de secretos replicada: Suma

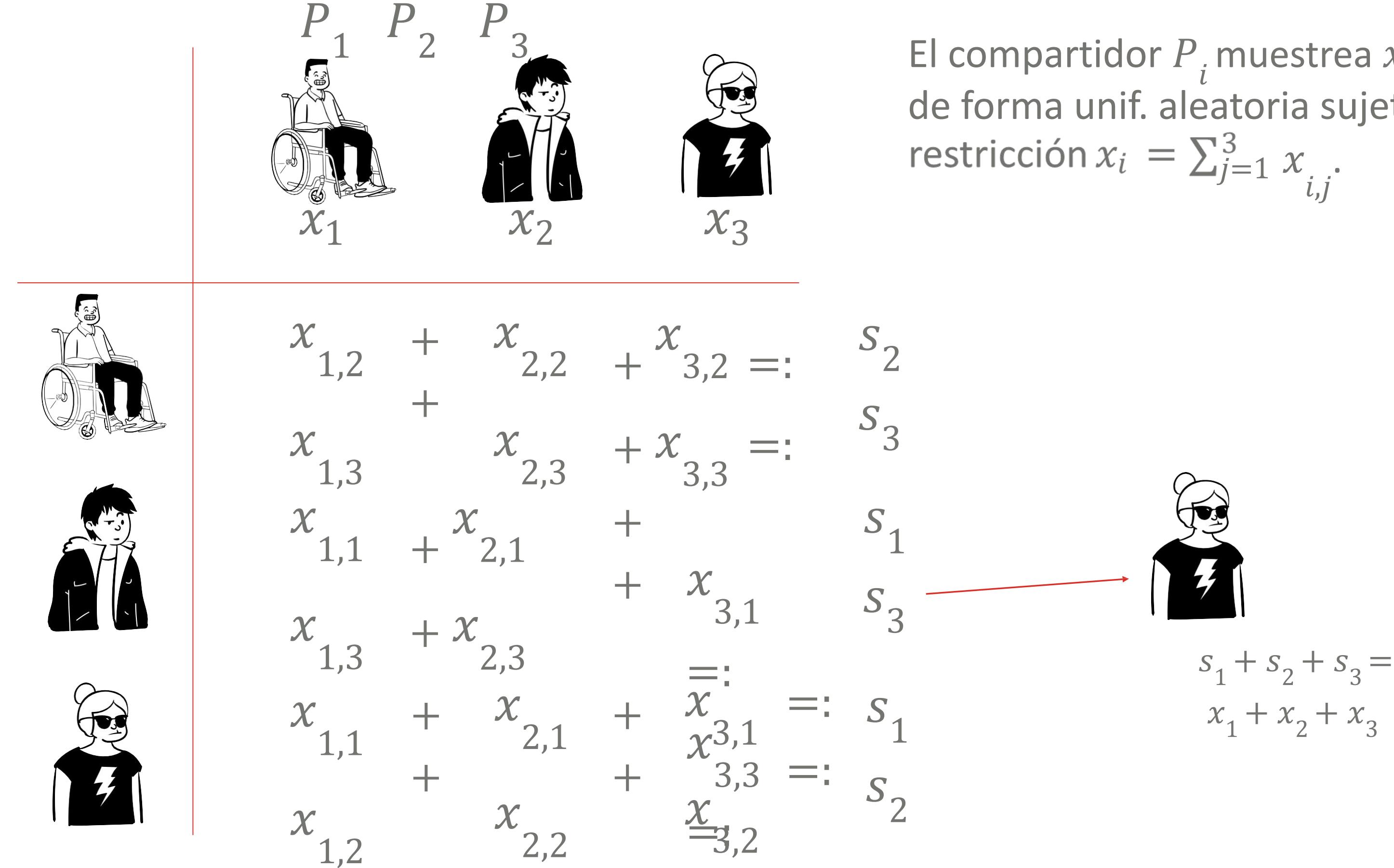


El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

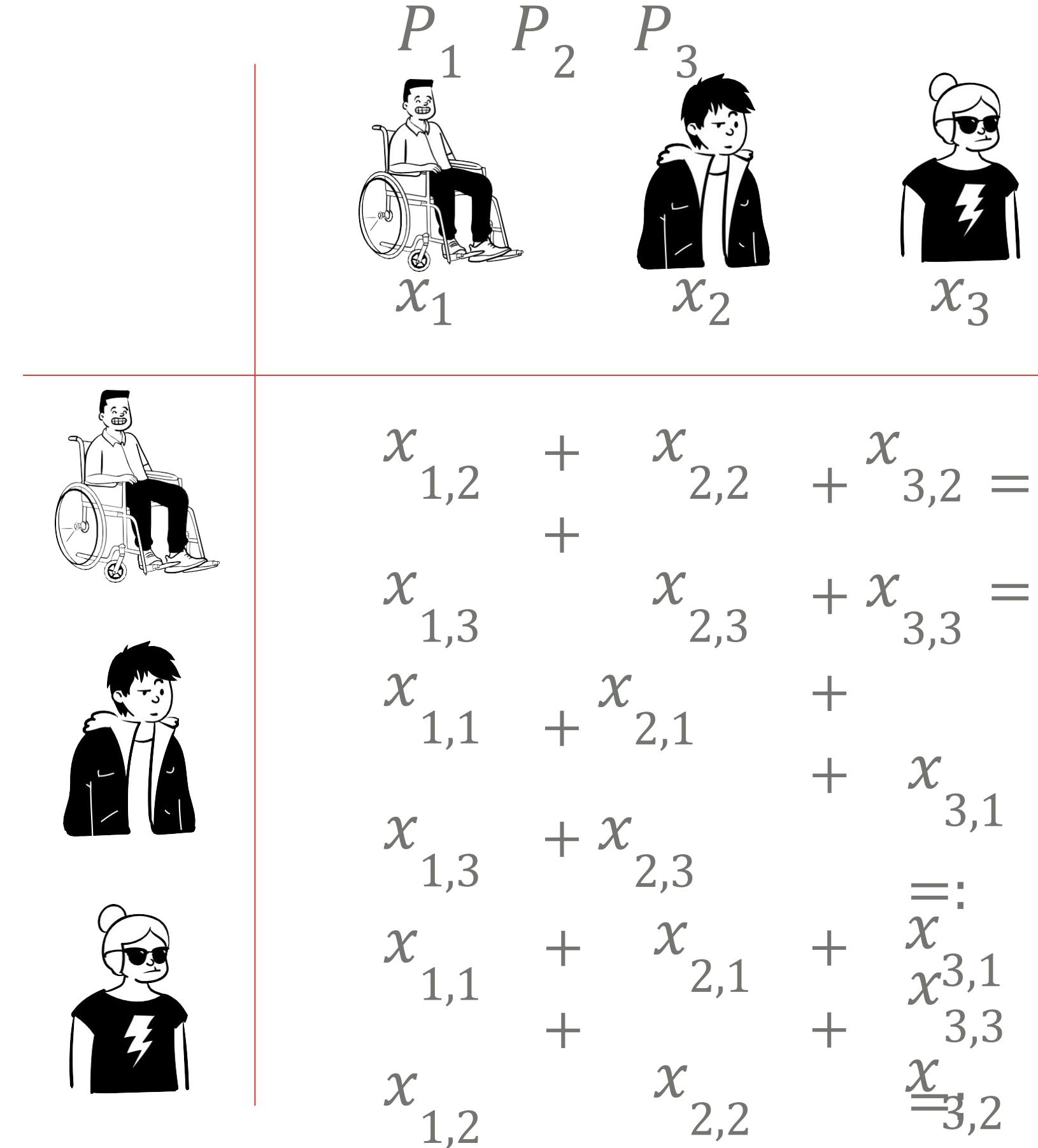


$$s_1 + s_2 + s_3 = \\ x_1 + x_2 + x_3$$

I Compartición de secretos replicada: Suma



I Compartición de secretos replicada: Suma



El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

s_2

s_3

s_1

s_3

s_1

s_1

s_2

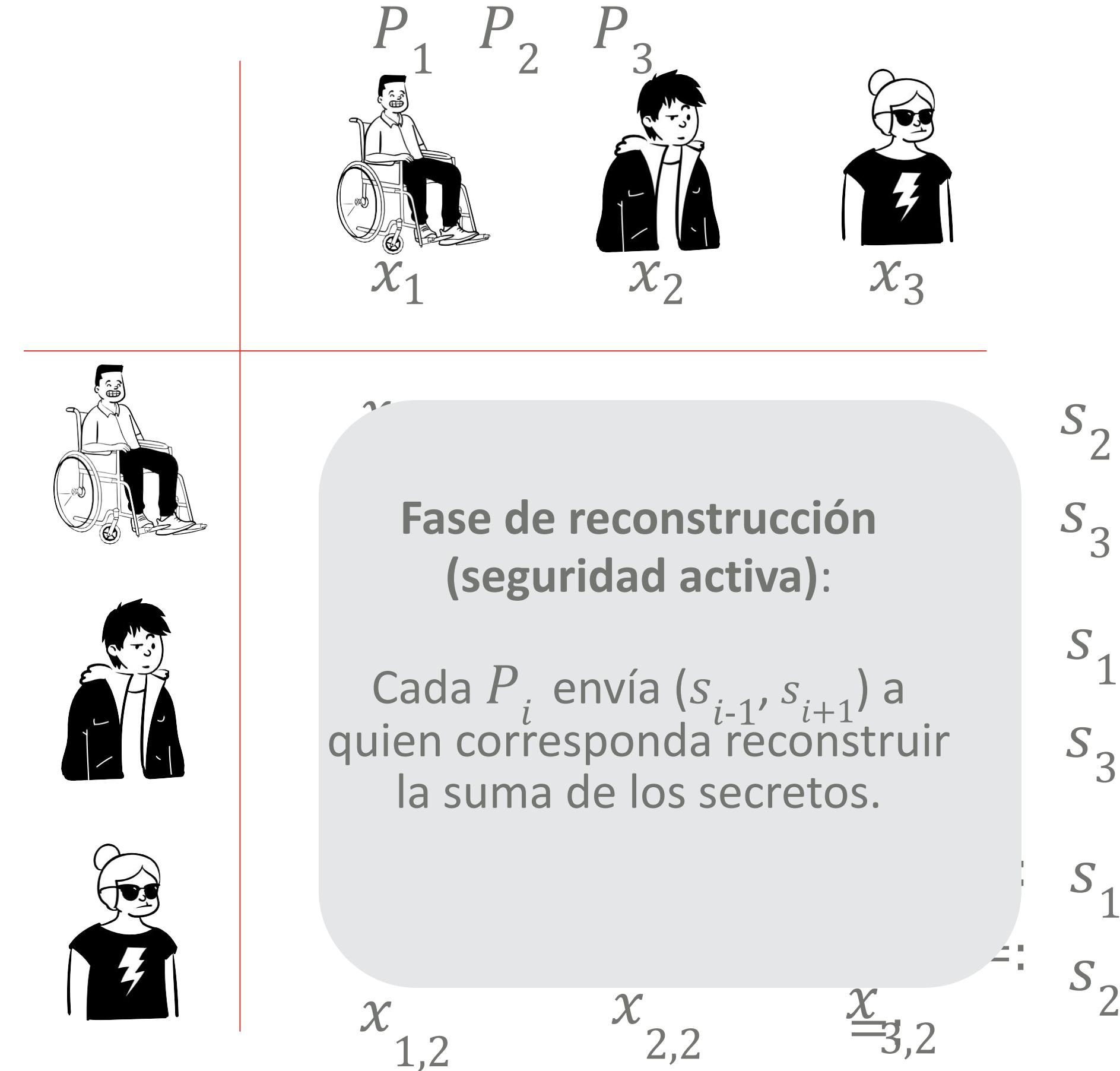
s_2

s_3

$s_1 + s_2 + s_3 =$

$x_1 + x_2 + x_3$

I Compartición de secretos replicada: Suma

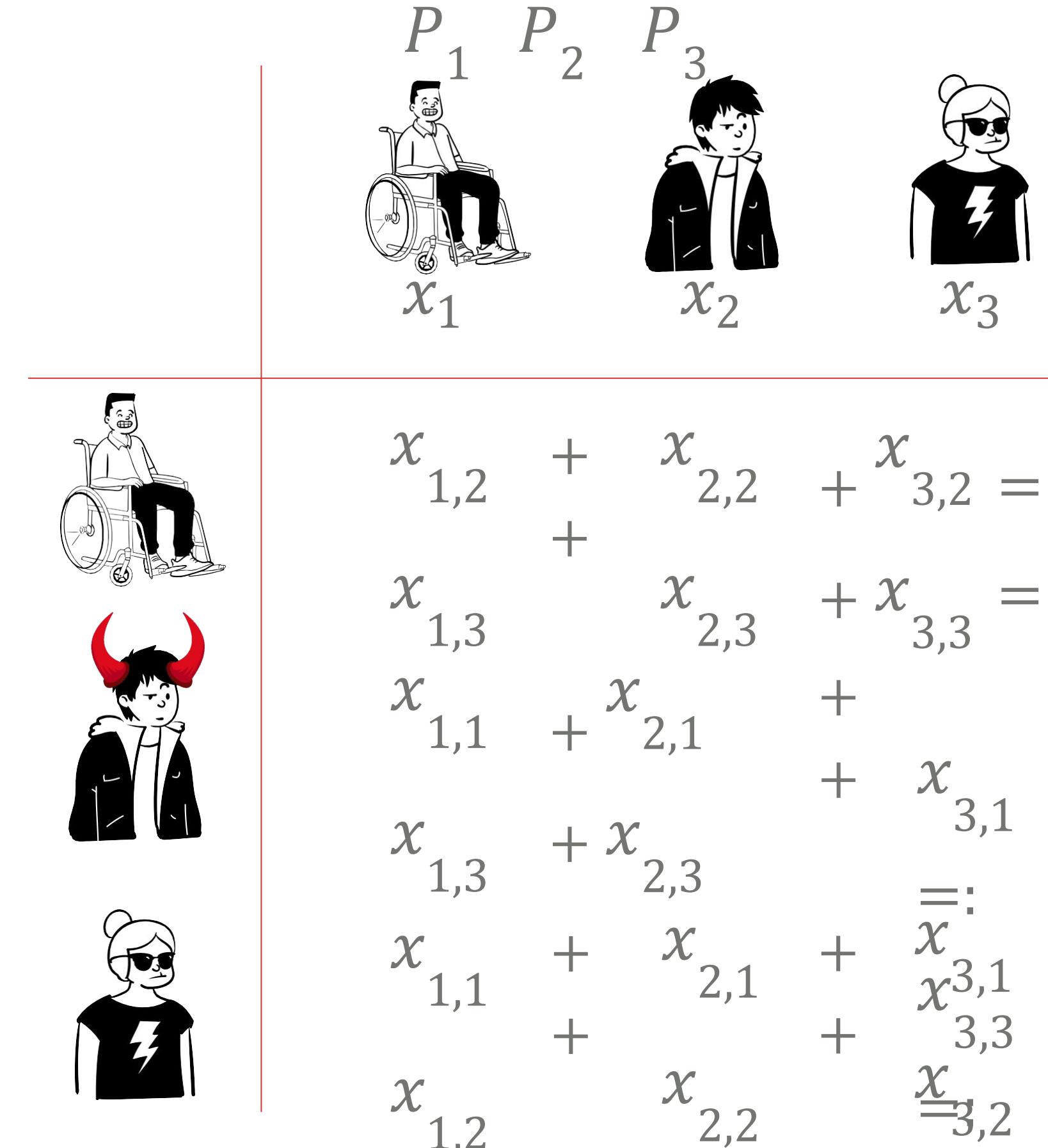


El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

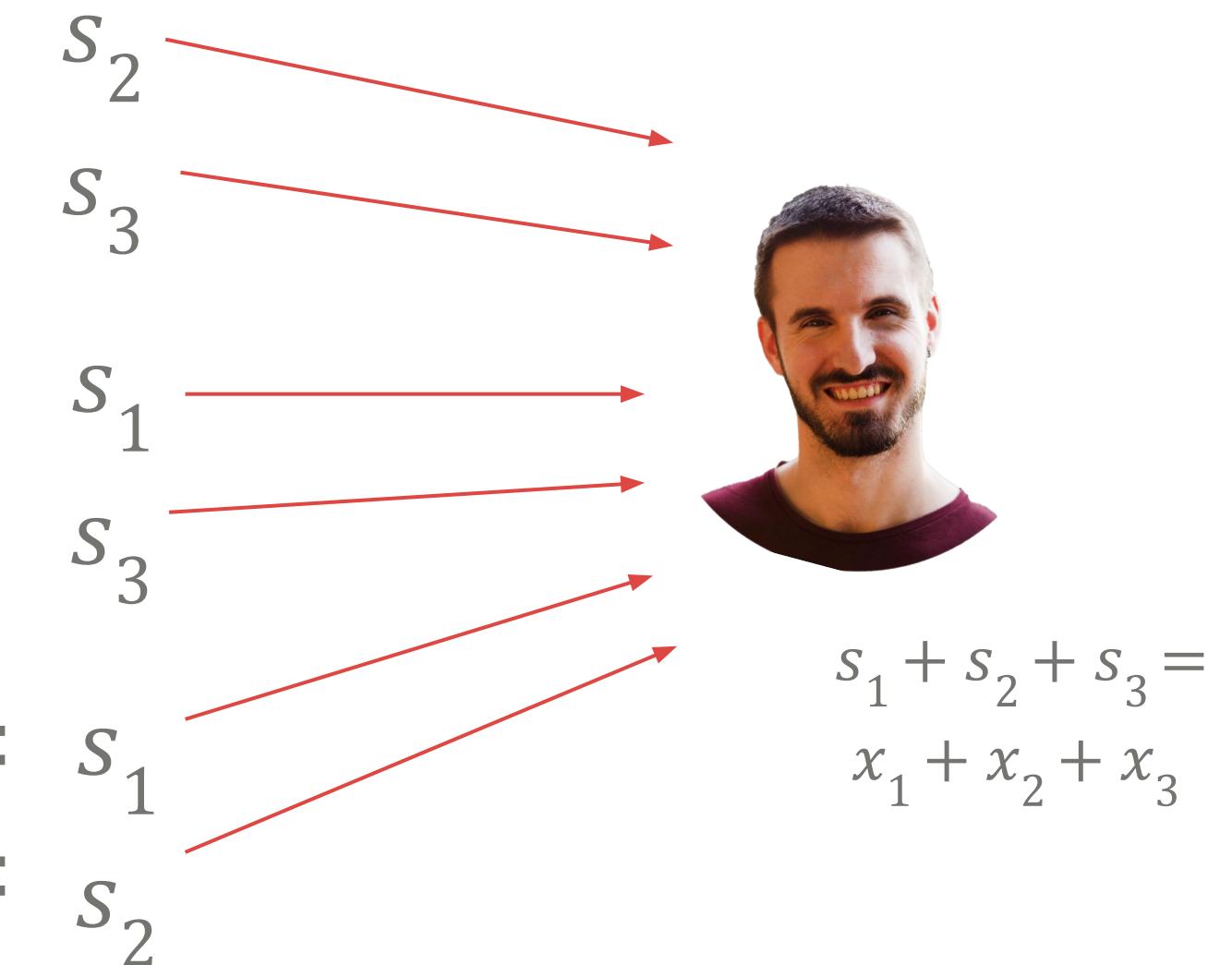
Idea Fundamental:
((s_2, s_3), (s_1, s_3), (s_1, s_2)) es una
compartición de secretos replicada
de $x_1 + x_2 + x_3$.

$$s_1 + s_3 + s_1 = \sum_{j=1}^3 x_{i,j} \\ x_1 + x_2 + x_3 =$$

I Compartición de secretos replicada: Suma

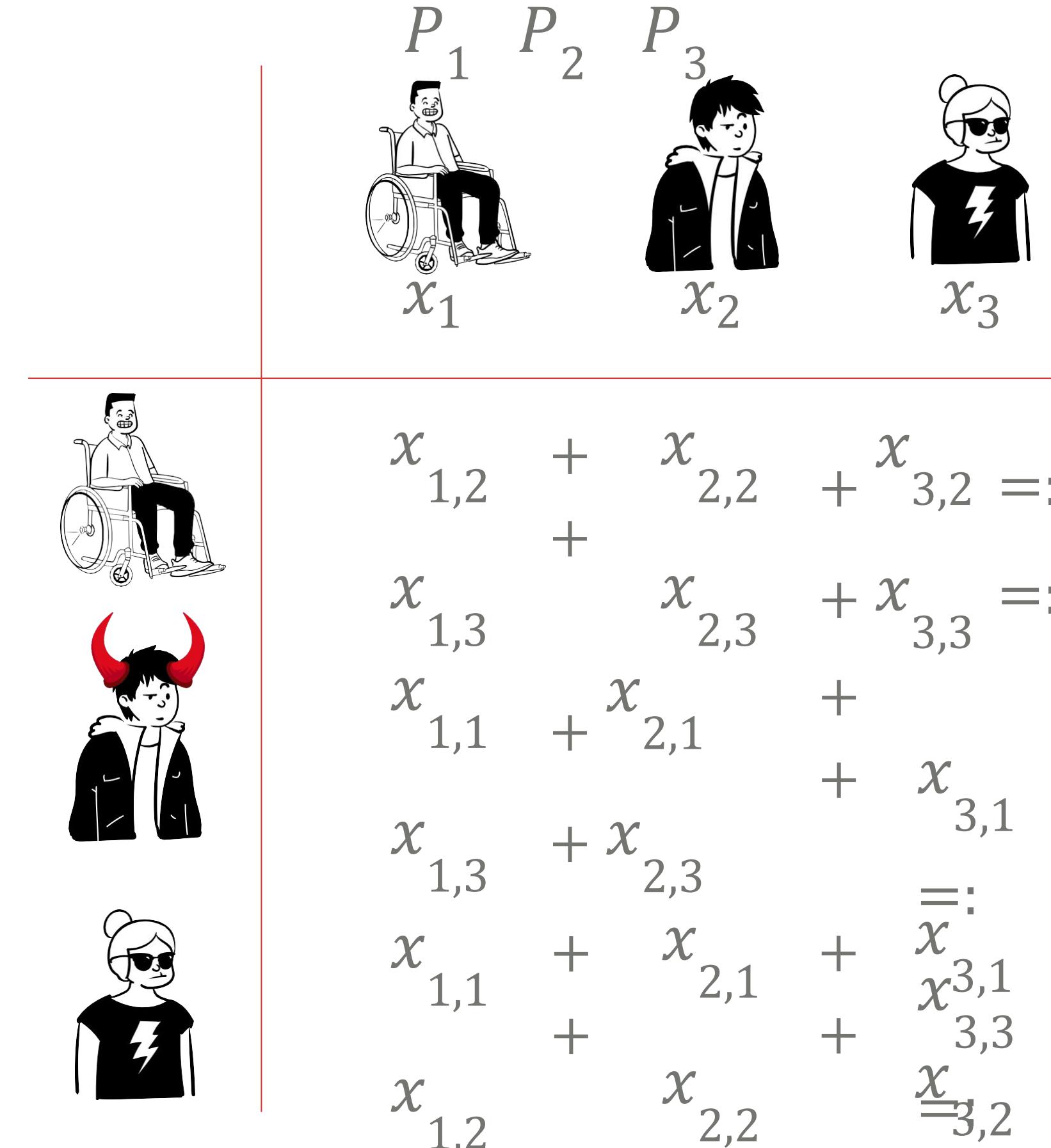


El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.

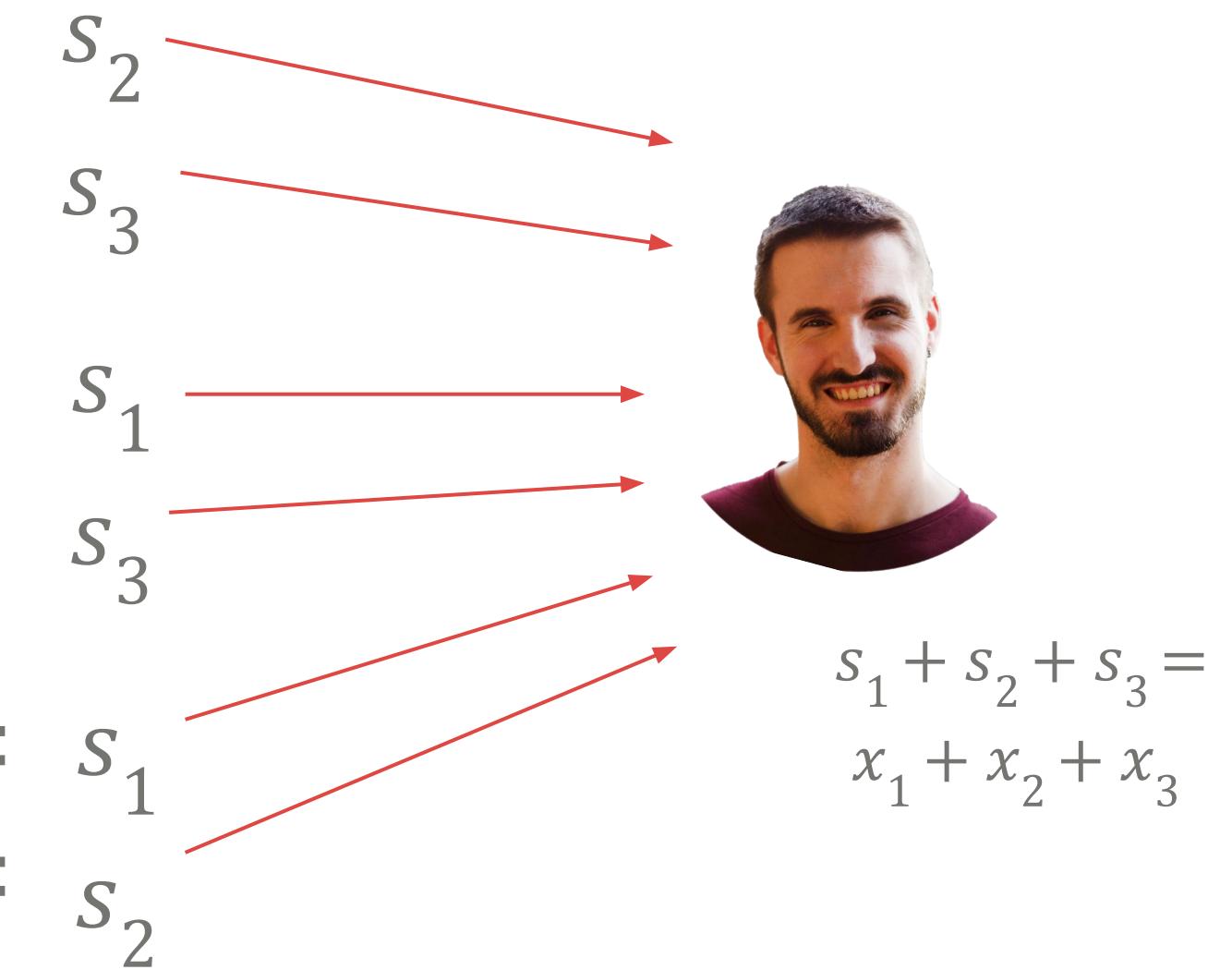


Cuál es el máximo problema que puede causar una entidad activamente corrupta?

I Compartición de secretos replicada: Suma

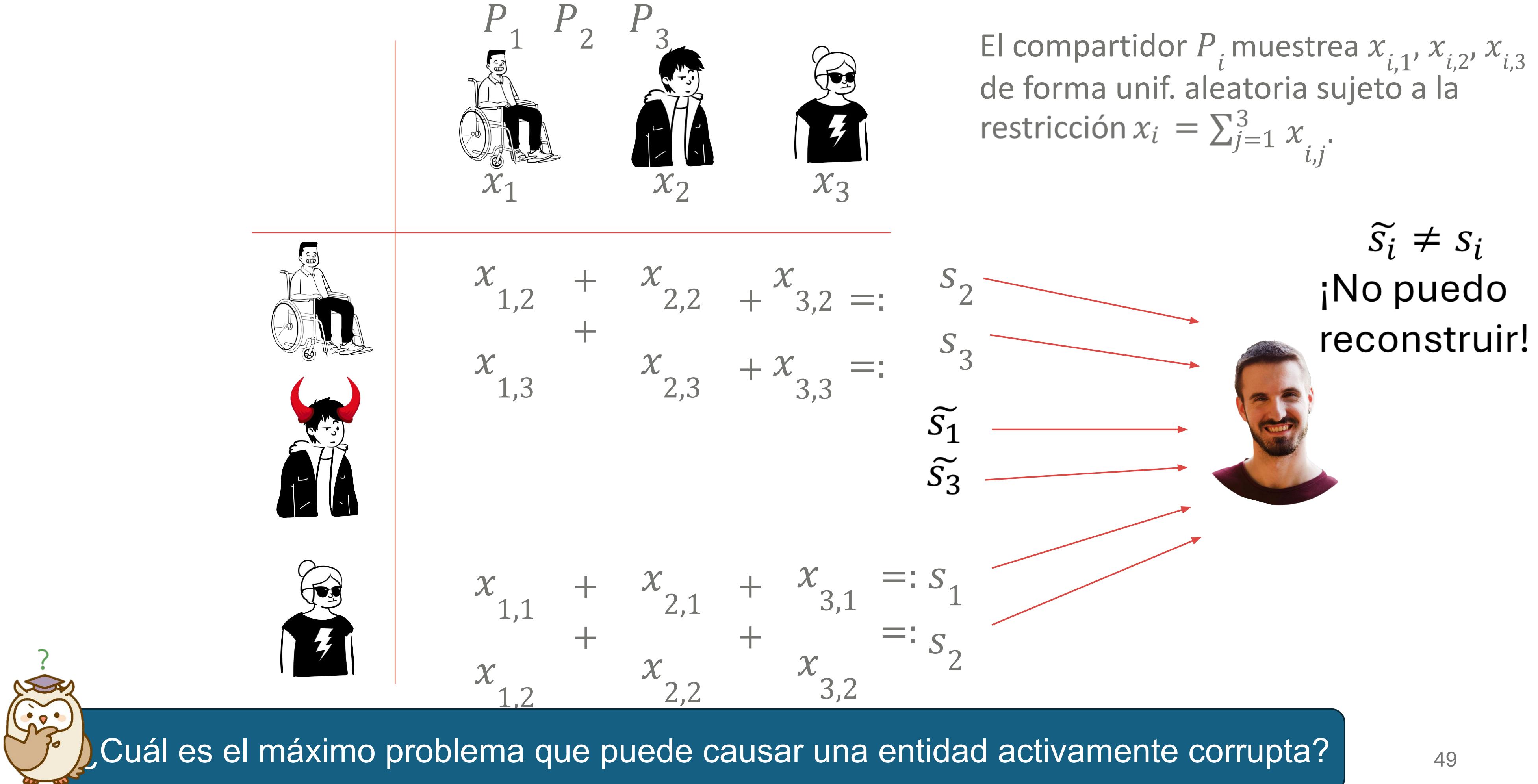


El compartidor P_i muestrea $x_{i,1}, x_{i,2}, x_{i,3}$ de forma unif. aleatoria sujeto a la restricción $x_i = \sum_{j=1}^3 x_{i,j}$.



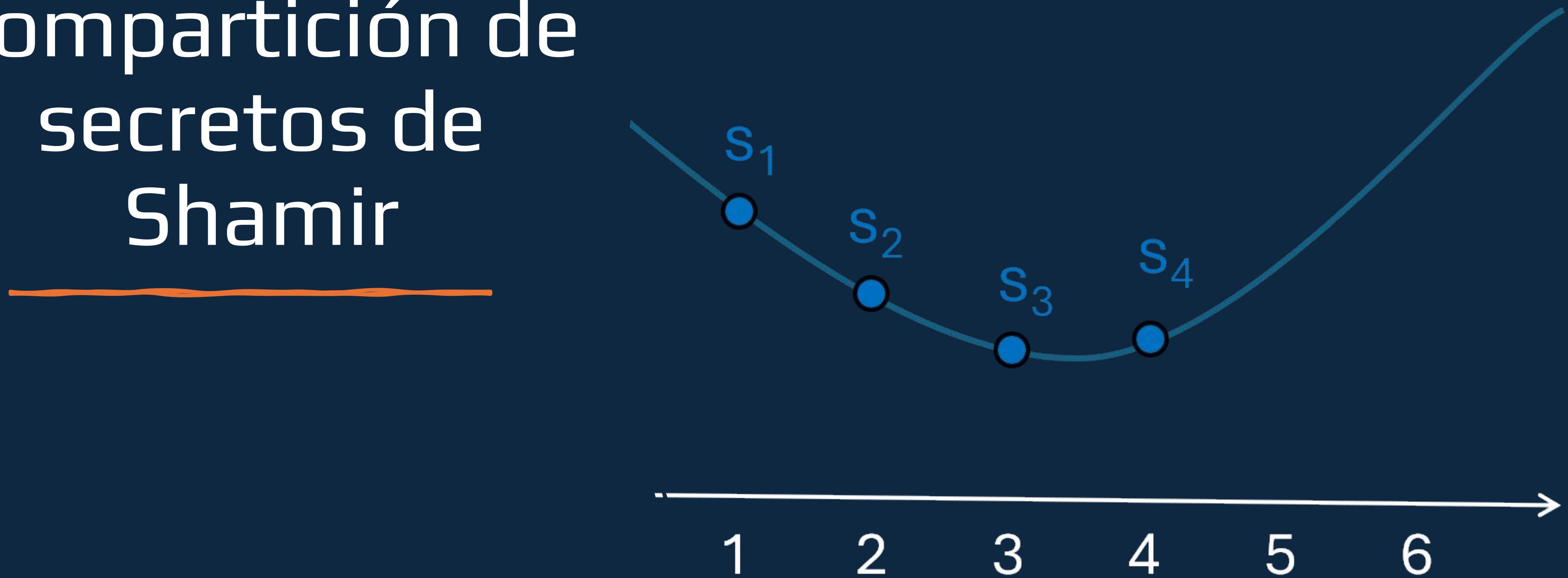
Cuál es el máximo problema que puede causar una entidad activamente corrupta?

I Compartición de secretos replicada: Suma



Cuál es el máximo problema que puede causar una entidad activamente corrupta?

Compartición de secretos de Shamir



|| Compartición de secretos de Shamir (n entidades)

Sea $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$; $\mathbb{Z}/p\mathbb{Z} = (0, 1, \dots, p - 1)$, p es un número primo, $p > n$.

1. Fase de compartición:

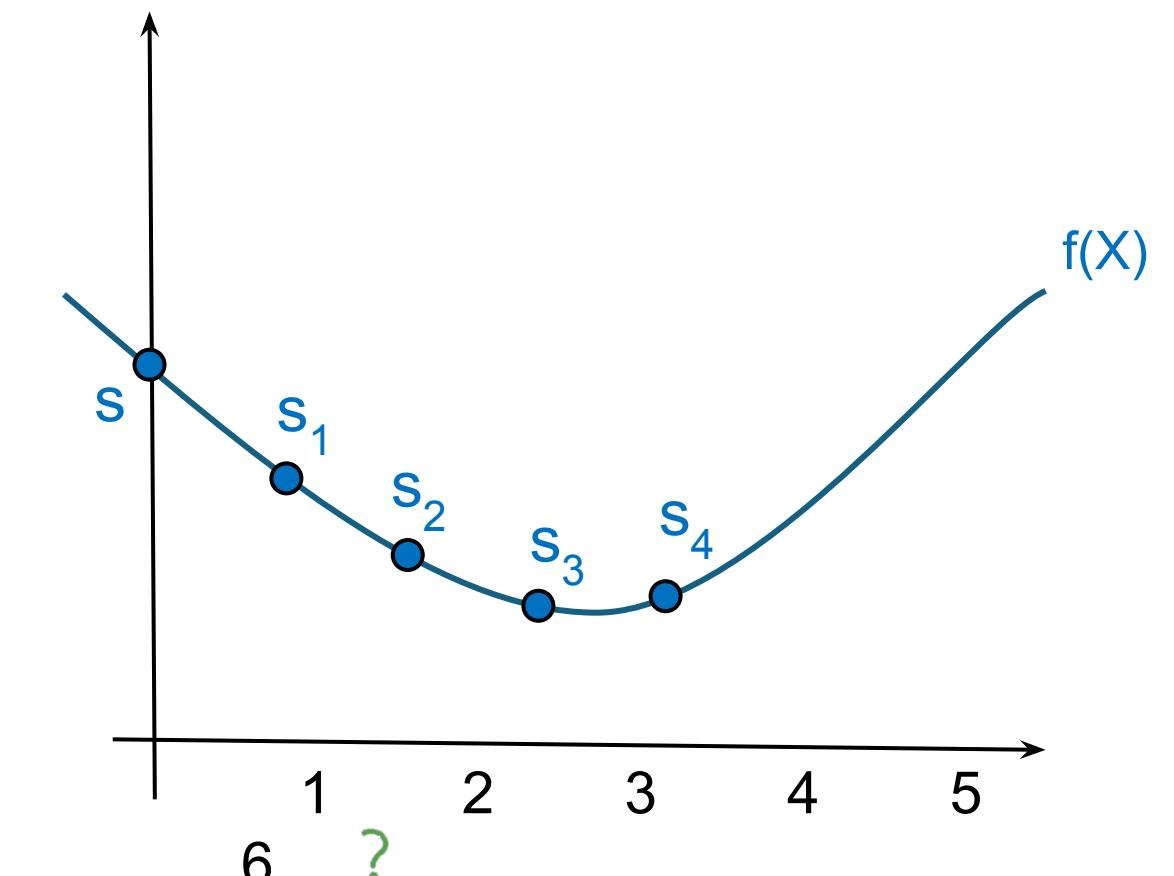
- Compartidor* escoge de forma unif. aleatoria $f \in \mathbb{F}_p[X]$ de grado t tal que $f(0) = s$.
- Compartidor* a cada P_i su parte $f(i) = s_i$.

2. Fase de reconstrucción:

- Cada P_i envía s_i a la entidad que quieren que reconstruya el secreto.
- Dicha entidad obtiene $f \in \mathbb{F}_p[X]$ mediante interpolación y recupera el secreto evaluando $f(0) = s$.



¿Cuál es el umbral t ? ¿Por qué es t -privado y $(t+1)$ -reconstruible?



¿Es lineal?

|| Compartición de secretos de Shamir



Pista: Matrices de Vandermonde

$$Van^{u \times v}(\alpha_1, \dots, \alpha_u) = \begin{bmatrix} \alpha_1^0 & \alpha_1^1 & \alpha_1^2 & \cdots & \alpha_1^{v-1} \\ \alpha_2^0 & \alpha_2^1 & \alpha_2^2 & \cdots & \alpha_2^{v-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_u^0 & \alpha_u^1 & \alpha_u^2 & \cdots & \alpha_u^{v-1} \end{bmatrix} \in \mathcal{M}_{u \times v}(\mathbb{F}_p)$$

Si $u = v$ y $\forall i \neq j, \alpha_i \neq \alpha_j$, entonces $Van^{u \times v}(\alpha_1, \dots, \alpha_u)$ es invertible.
Además, lo son también todas sus submatrices cuadradas.

Sea $f(X) = \sum_{i=0}^t f_i \cdot X^i$ el polinomio en $\mathbb{F}_p[X]$ de grado $\leq t$.

$$(f(\alpha_1), \dots, f(\alpha_{t+1})) = Van^{u \times v}(\alpha_1, \dots, \alpha_{t+1}) \cdot (f_0, \dots, f_t).$$

Implica: Linearidad (es más, isomorfismo), t-privacidad, (t+1) reconstruibilidad.

Pros/Cons de la compartición de secretos de Shamir

VENTAJAS

- El tamaño de cada parte es igual al tamaño del secreto.
- Tiene propiedades multiplicativas (siguientes diapositivas).
- Es equivalente a un código de Reed Solomon, donde se reparte un símbolo a cada entidad P_i . Por lo tanto, en presencia de un Adversario activo y para valores adecuados del umbral t , se pueden explotar las propiedades de detección y corrección de errores (para más información, consultar p.ej. [Esc22]).

INCONVENIENTES

- En comparación con la compartición de secretos aditiva o replicada, la reconstrucción es algo costosa a nivel computacional.

Referencias y lecturas

| Referencias y lecturas adicionales

- [Esc22] (Inglés) Daniel Escudero “**An Introduction to Secret-Sharing-Based Secure Multiparty Computation**” <https://eprint.iacr.org/2022/062.pdf>
- (Español) Curso Criptografía UNAL 2023:
<https://www.youtube.com/playlist?list=PLeld-Hlf3EnrwZnvOT4IH5-2a-6HRaTG0>
- Awesome MPC: <https://github.com/rdragos/awesome-mpc>
- (Inglés) Algunos despliegues de productos de MPC: <https://mpc.cs.berkeley.edu/>