Protocolli crittografici

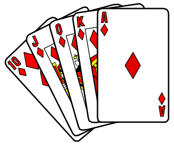
Clemente Galdi

Dipartimenti di Scienze Fisiche
Università di Napoli "Federico II"

c.galdi@na.infn.it

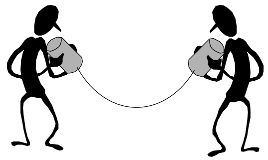
Protocolli crittografici

Lancio di una moneta 

Poker 

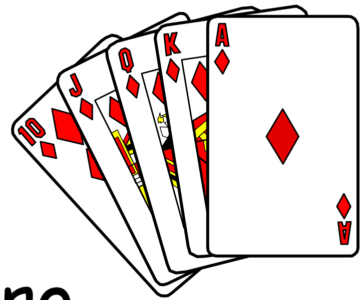
Moneta elettronica 

Elezioni 

Condivisione di segreti 

Email certificata 

Mental Poker



- Poker senza carte, con giocatori "curiosi" ma "onesti"
- Tre giocatori: **A**nnarella, **B**iagio, **C**iro
- Cifratura e decifratura commutative:

$$D(E(x,k_1),k_2) = E(D(x,k_2),k_1)$$

- Esempio: RSA con lo stesso modulo
  - Da implemetare con "cura"
  - Stesso modulo -> stessi valori di p e q

Mental Poker: B ottiene 5 carte

A | **B**

Cifro e permuto le 52 carte

$E(x_1,k_A),\dots,E(x_{52},k_A)$

$$E(x_4,k_A),\dots,E(x_{32},k_A) \longrightarrow$$

Scelgo 5 carte
e le cifro

$$E(E(x_5,k_A),k_B),\dots,E(E(x_2,k_A),k_B) \longleftarrow$$

Decifro i 5 valori

$$D(E(E(x_5,k_A),k_B)\ k_A),\dots,D(E(E(x_2,k_A),k_B)\ k_A) \longrightarrow$$

Mental Poker: B ottiene 5 carte

A		B

Cifro e permuto le 52 carte

$E(x_1,k_A),\ldots,E(x_{52},k_A)$

$$E(x_4,k_A),\ldots,E(x_{32},k_A) \longrightarrow$$

Scelgo 5 carte e le cifro

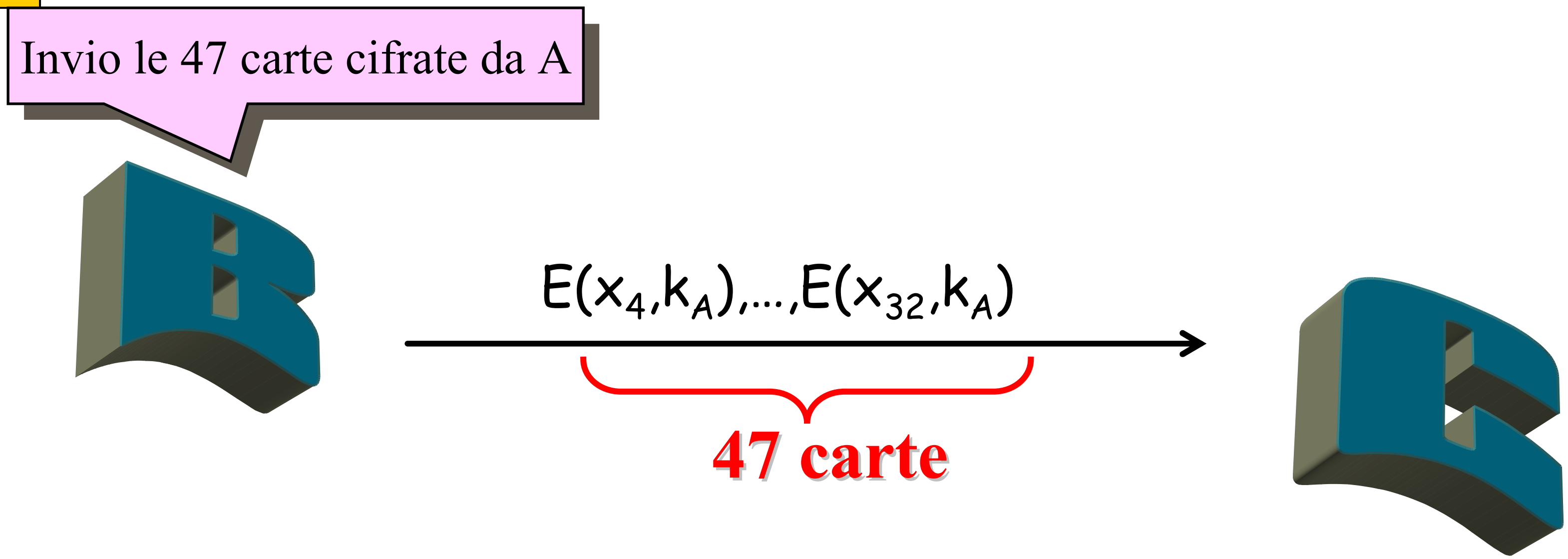
$$\longleftarrow E(E(x_5,k_A),k_B),\ldots,E(E(x_2,k_A),k_B)$$

Decifro i 5 valori

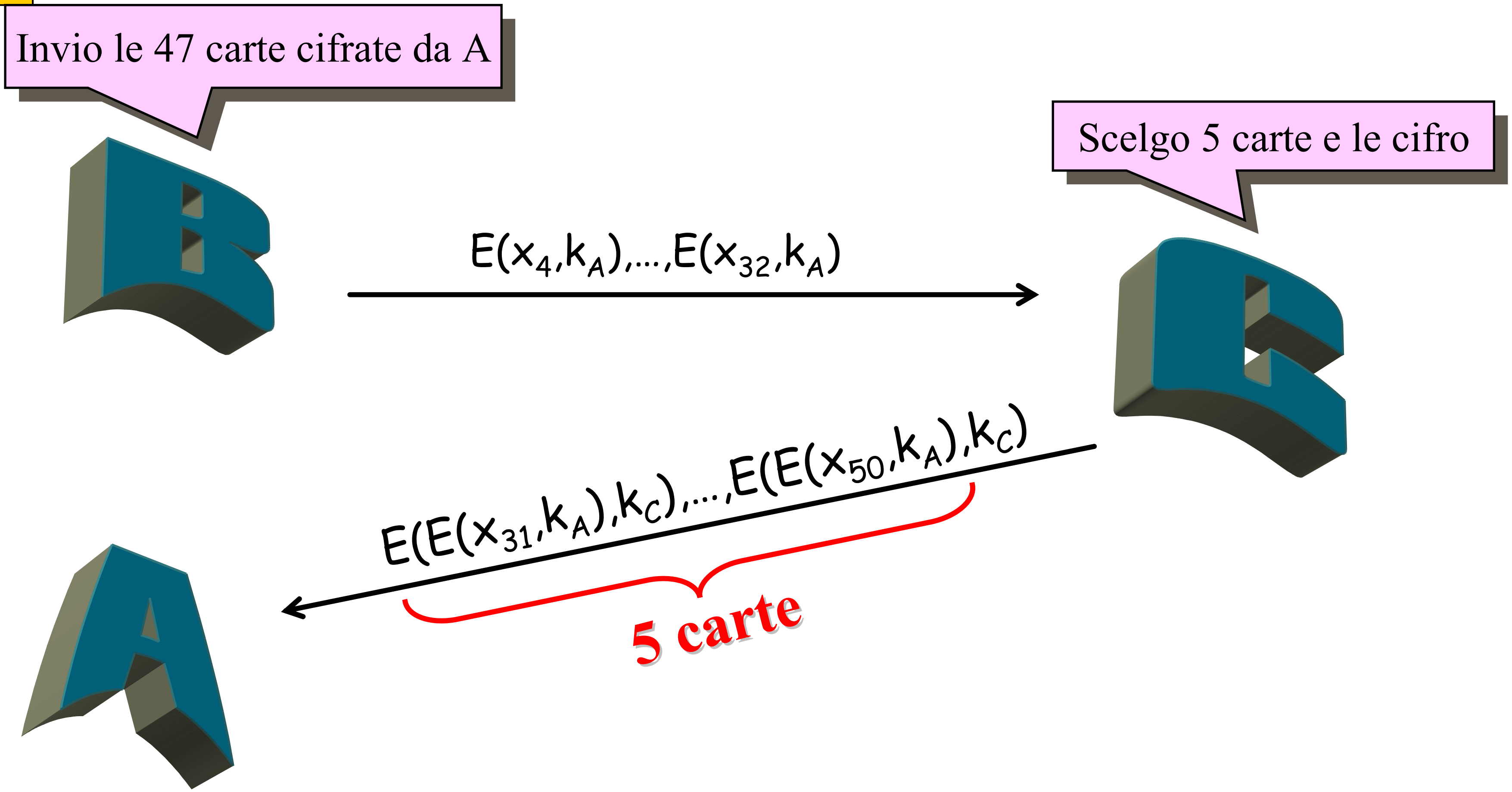
$$E(x_5,k_B),\ldots,E(x_2,k_B) \longrightarrow$$

$x_5,\ldots,x_2$

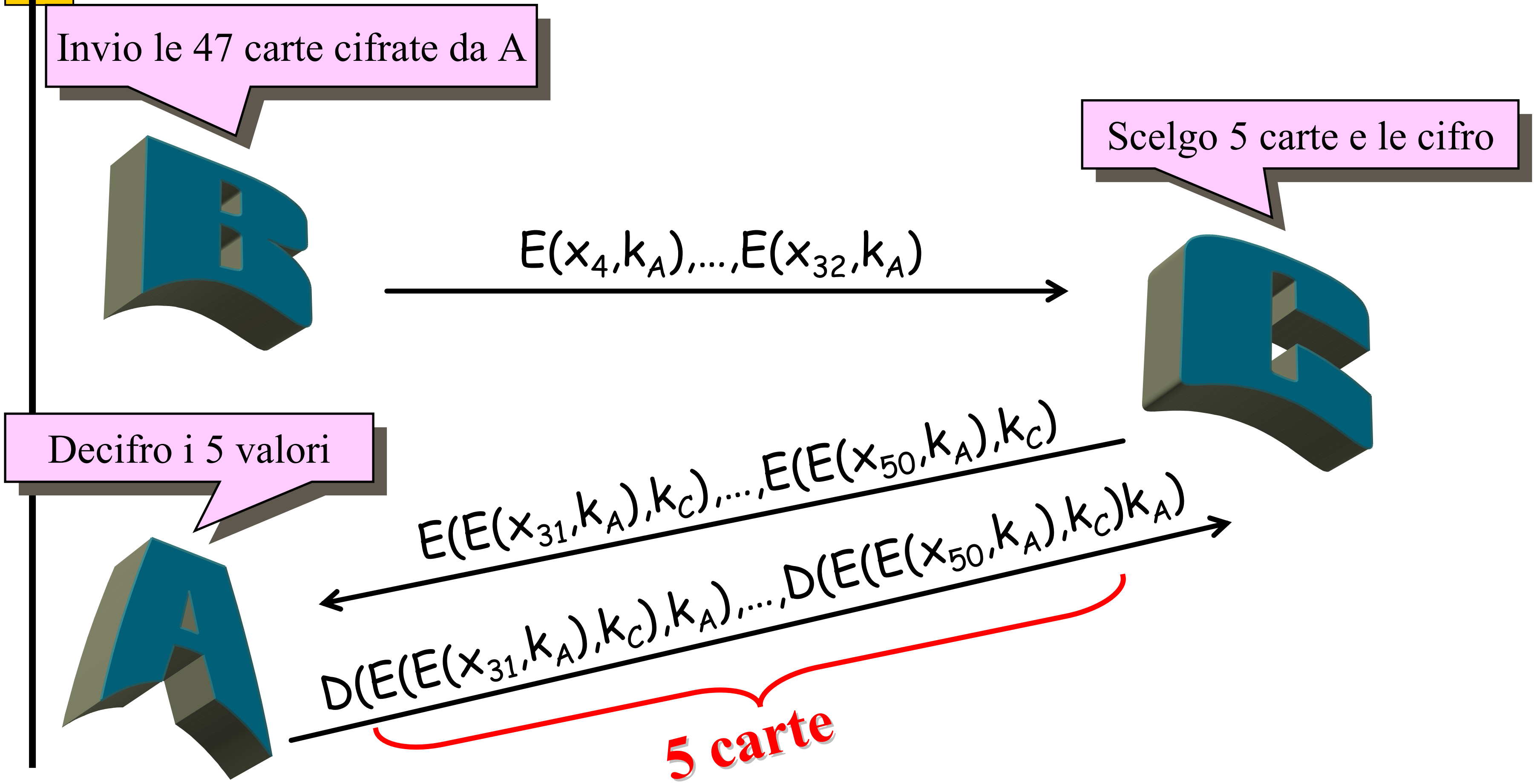
Mental Poker: C ottiene 5 carte



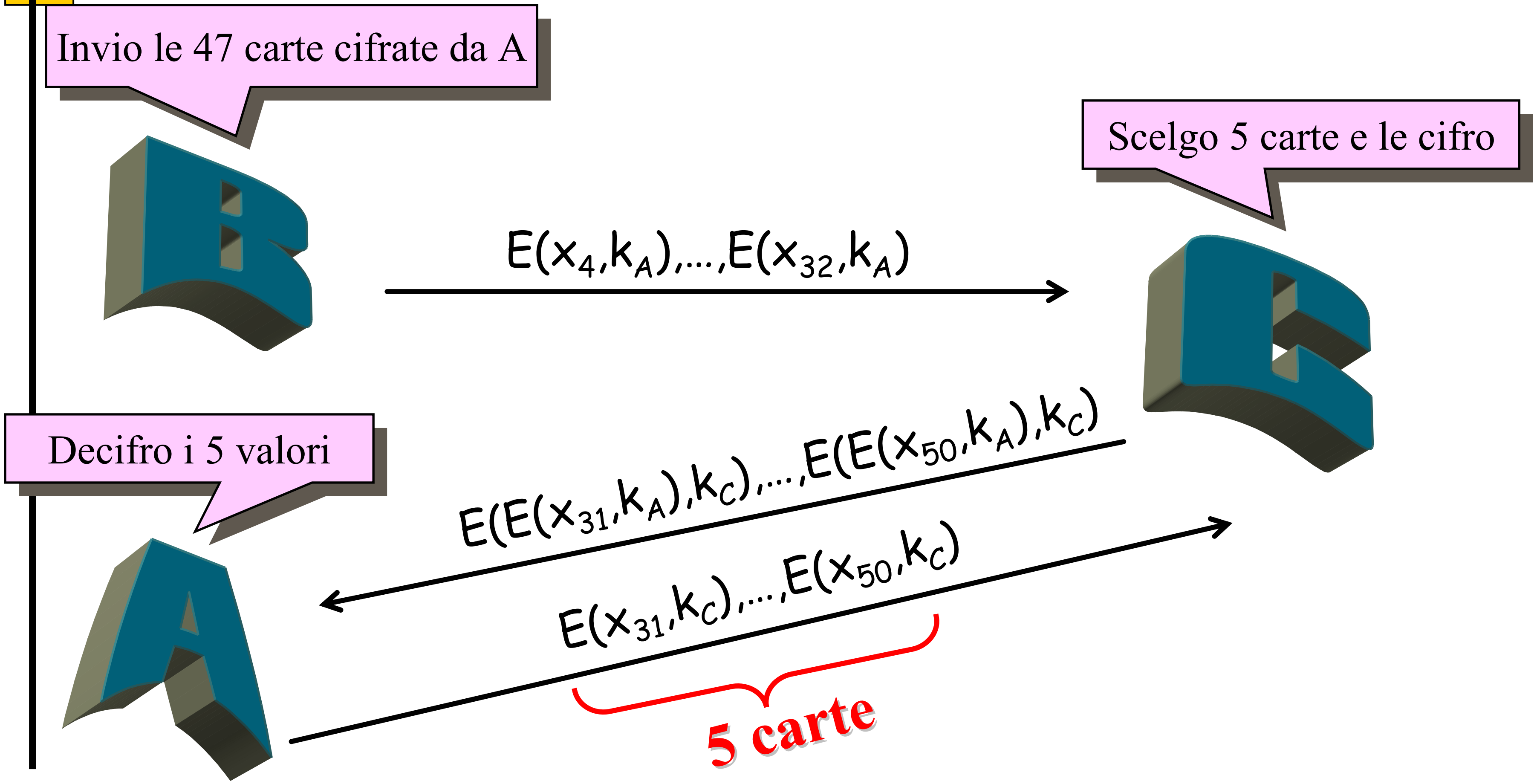
Mental Poker: C ottiene 5 carte



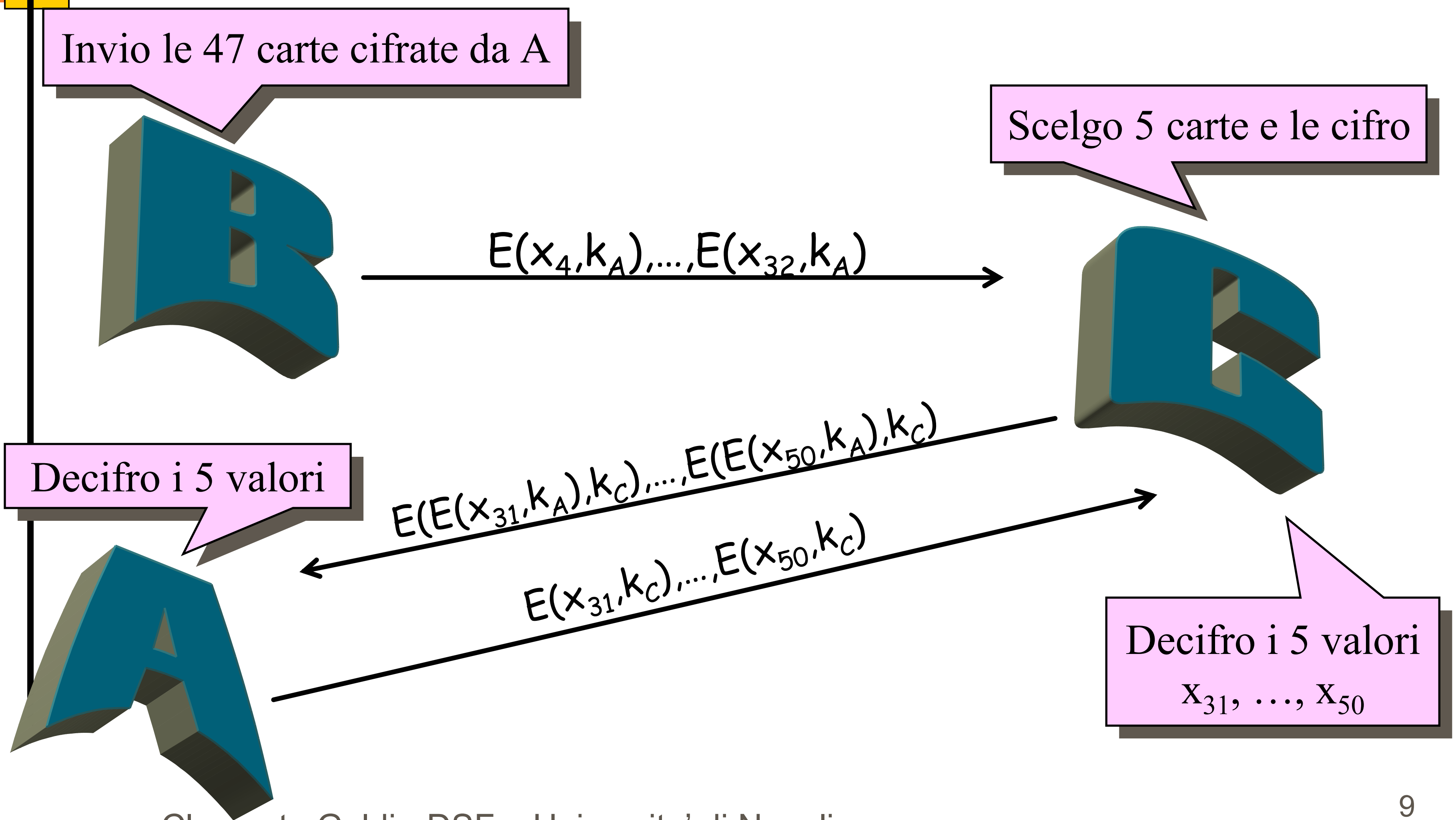
Mental Poker:
C ottiene 5 carte



Mental Poker: C ottiene 5 carte



Mental Poker: C ottiene 5 carte



Mental Poker: A ottiene 5 carte

Scelgo ed invio 5 tra le 42 carte cifrate da A

B

$$E(x_{11},k_A),\ldots,E(x_{45},k_A)$$

5 carte

A

Decifro i 5 valori $x_{11},\ldots,x_{45}$

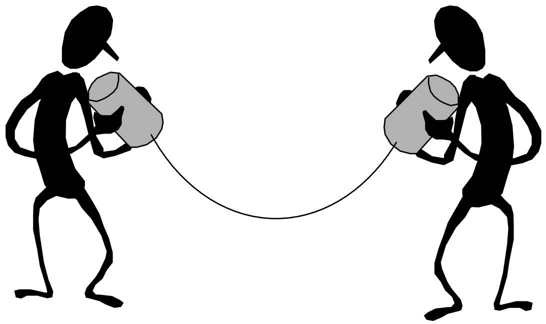
Mental Poker

- Giocatori "curiosi" ma "onesti"
- Se non fossero "onesti"
  - Uso di prove *zero-knowledge*
  - Alla fine, tutti rivelano le chiavi utilizzate
  - Alla fine, solo il vincitore rivela le chiavi utilizzate

Condivisione di segreti

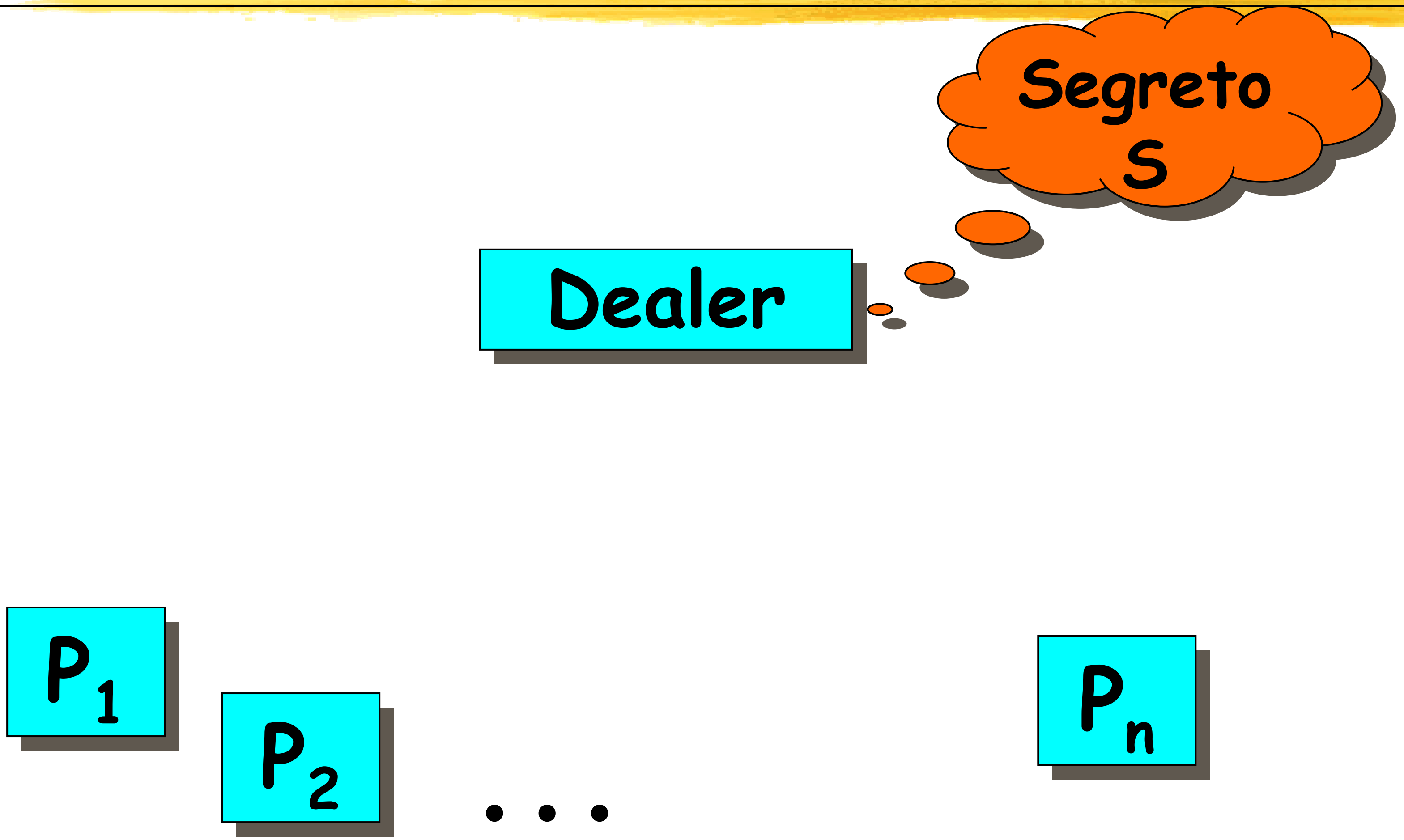
Un dealer vuole condividere un segreto S tra n partecipanti in modo che:

- k o più partecipanti possano ricostruire S
- k-1 o meno partecipanti non hanno alcuna informazione su S

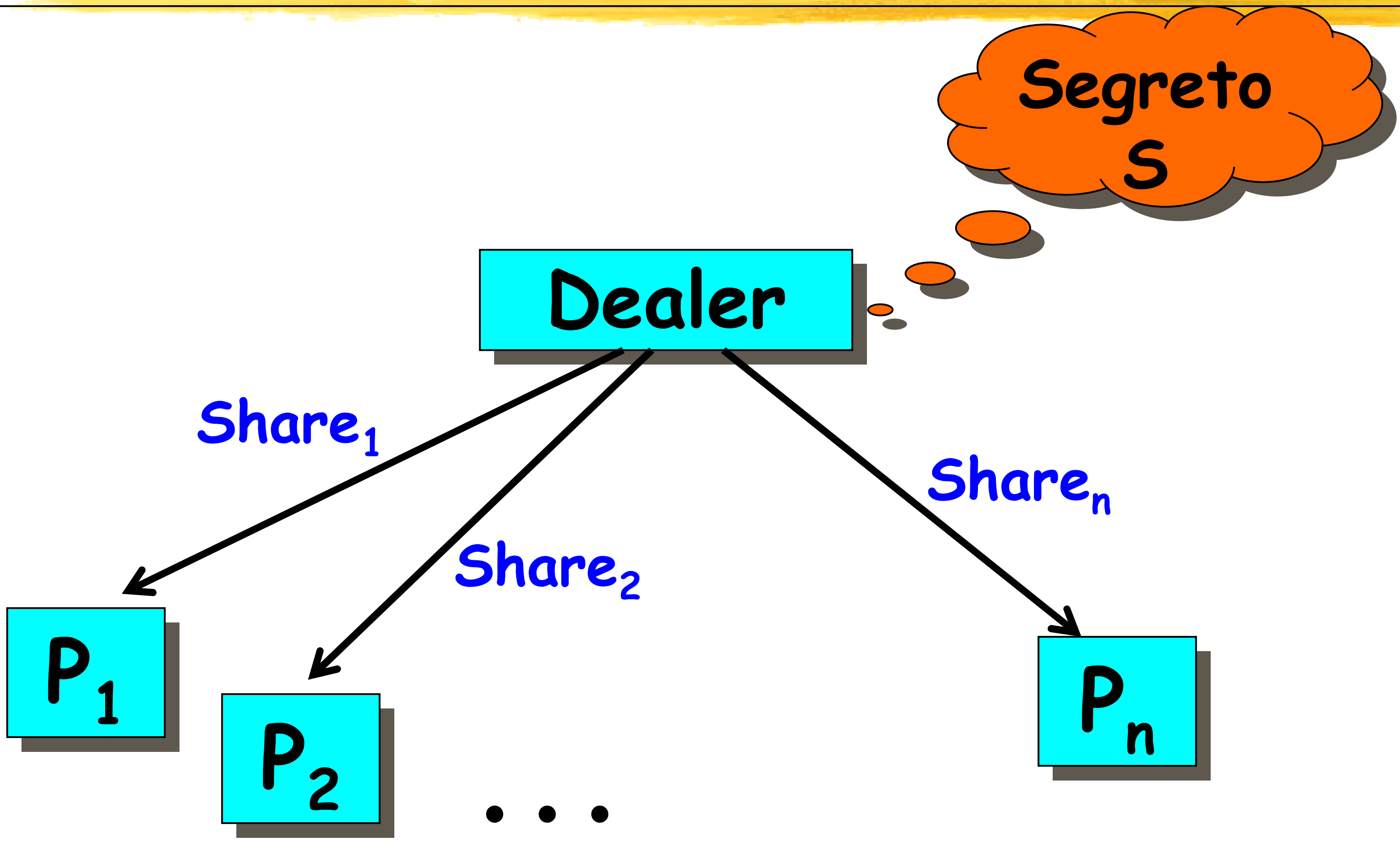


[Adi Shamir, 1979]

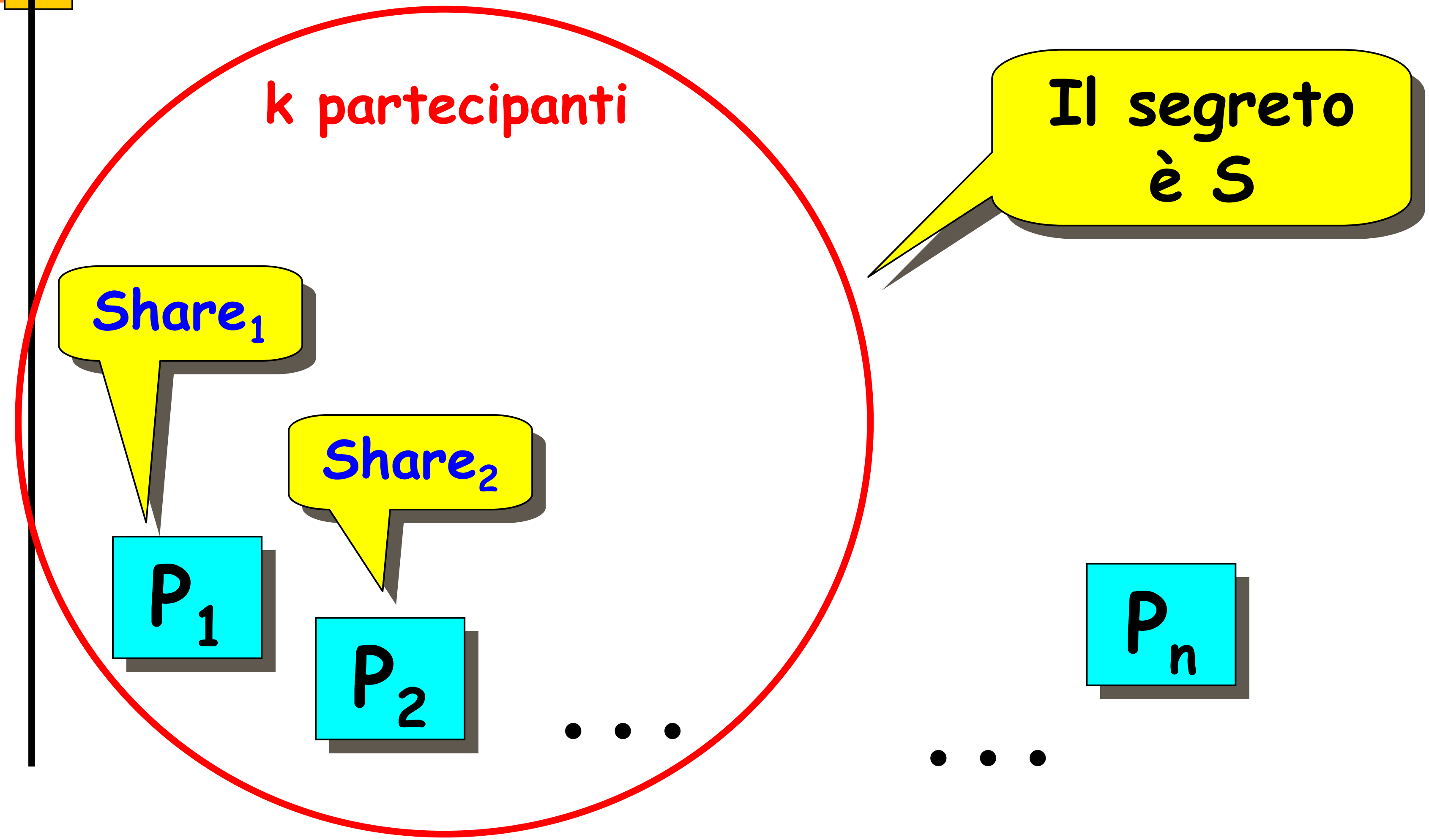
Scenario



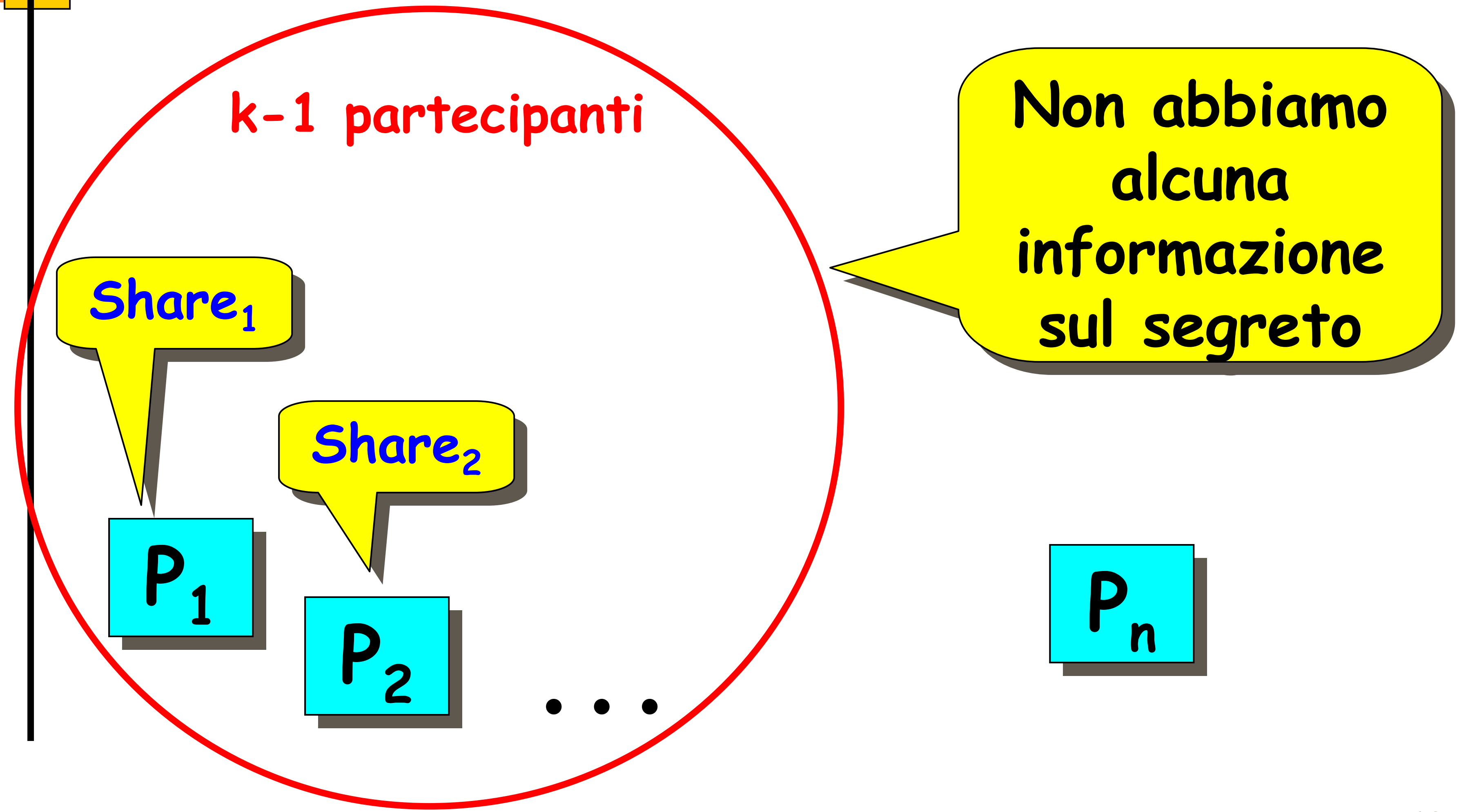
Distribuzione del segreto



Ricostruzione del segreto



Ricostruzione del segreto

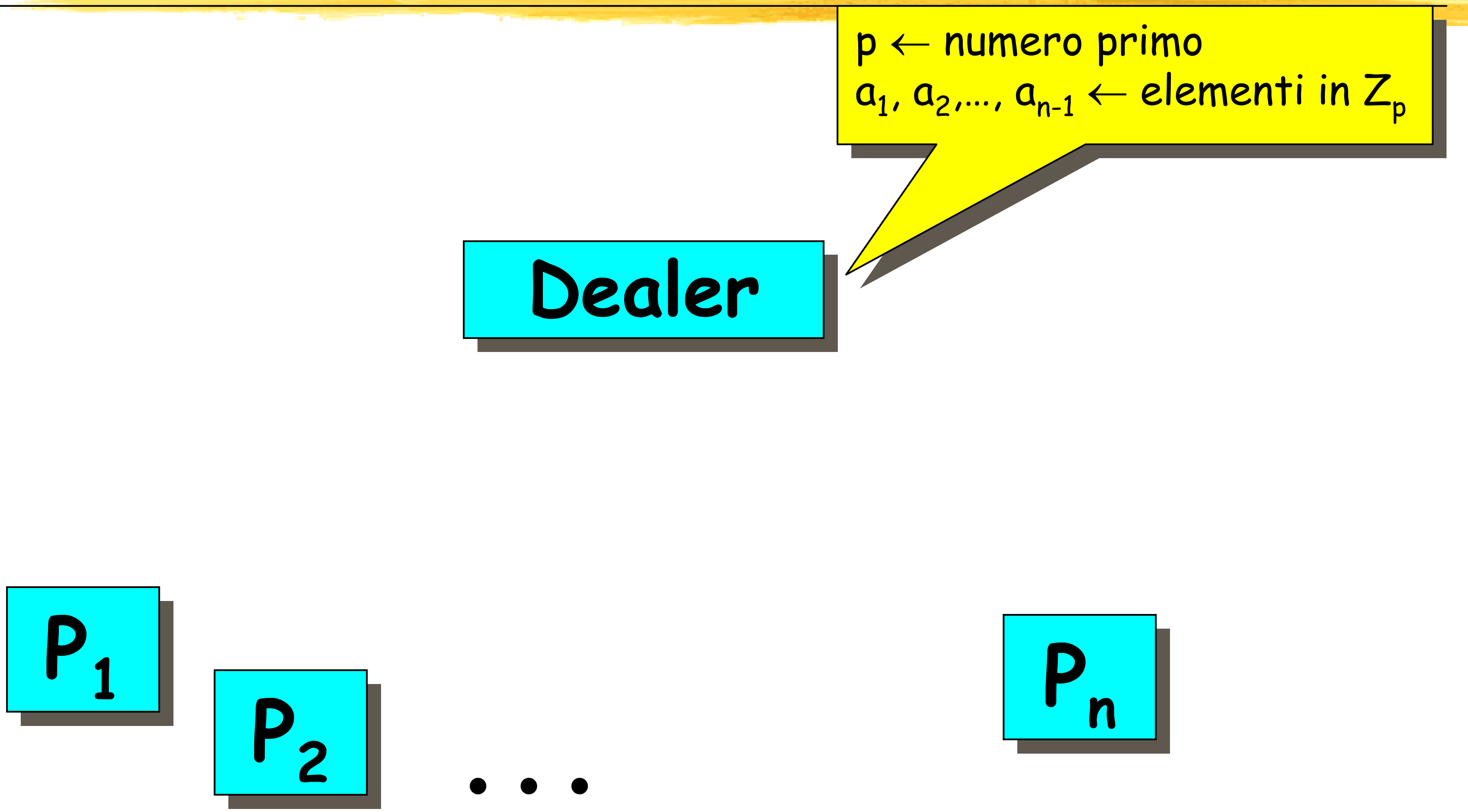


Condivisione di segreti

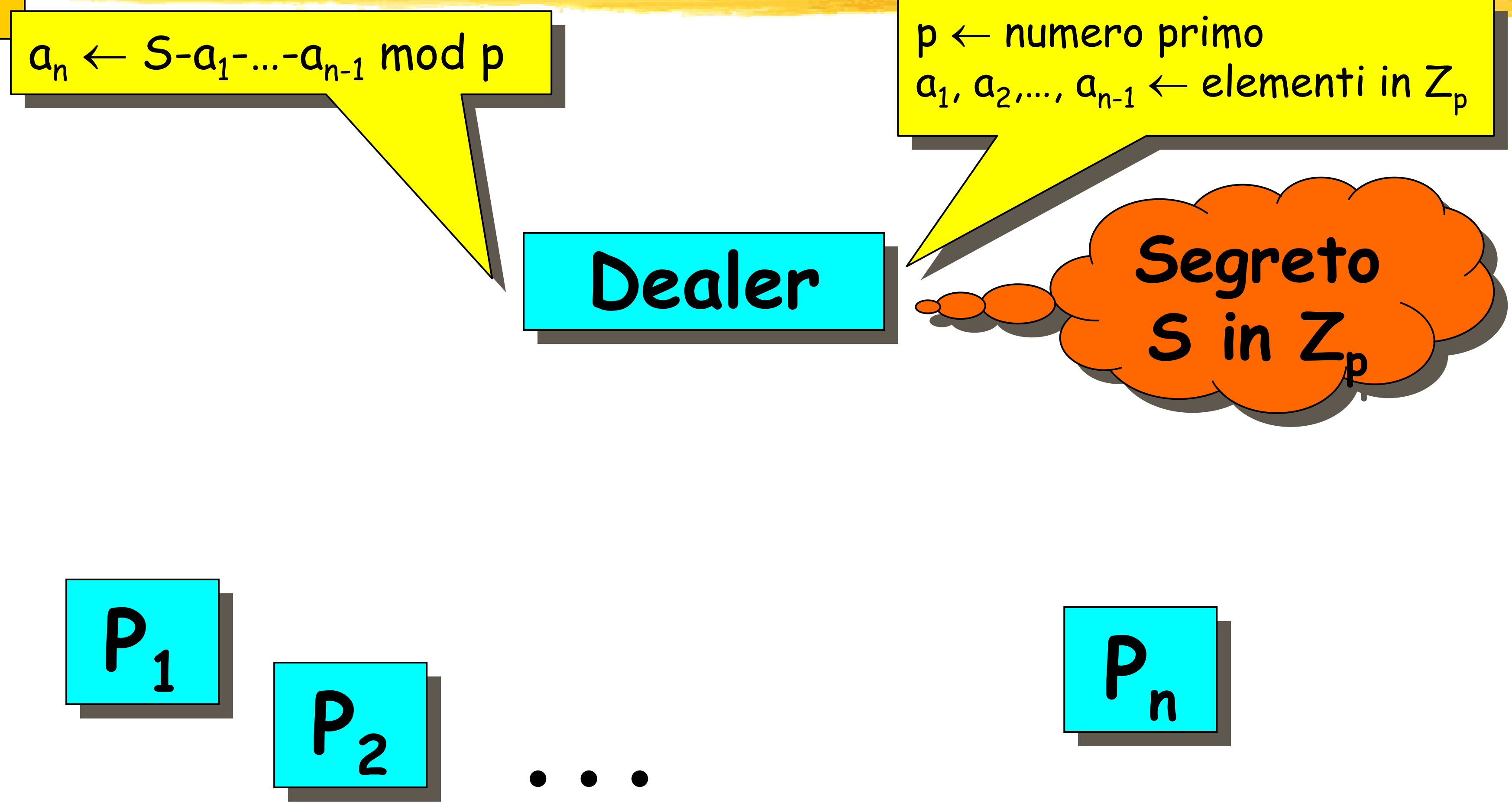
Vedremo:

- Schema (n,n)
- Schema (k,n)

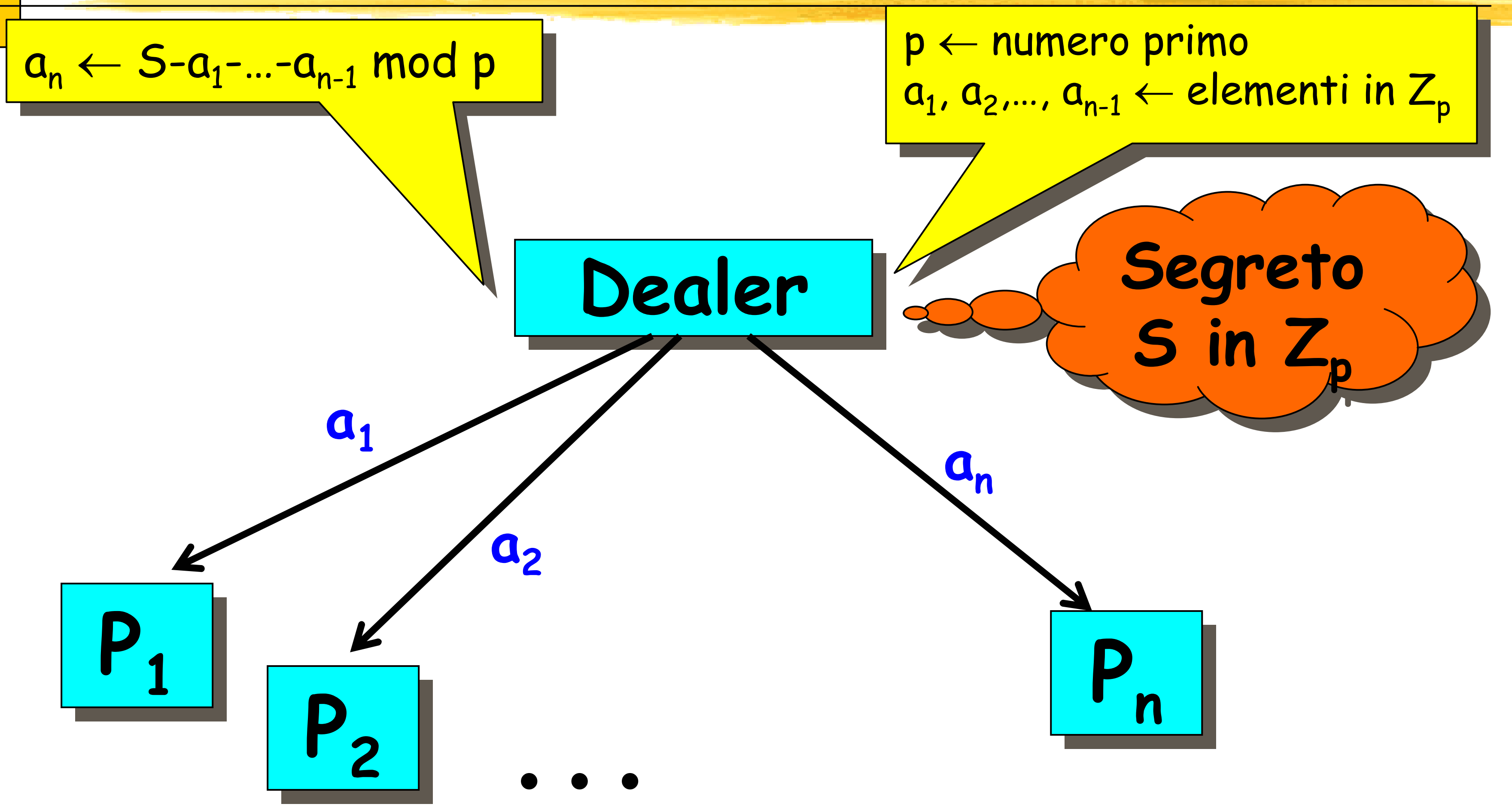
Inizializzazione schema (n,n)



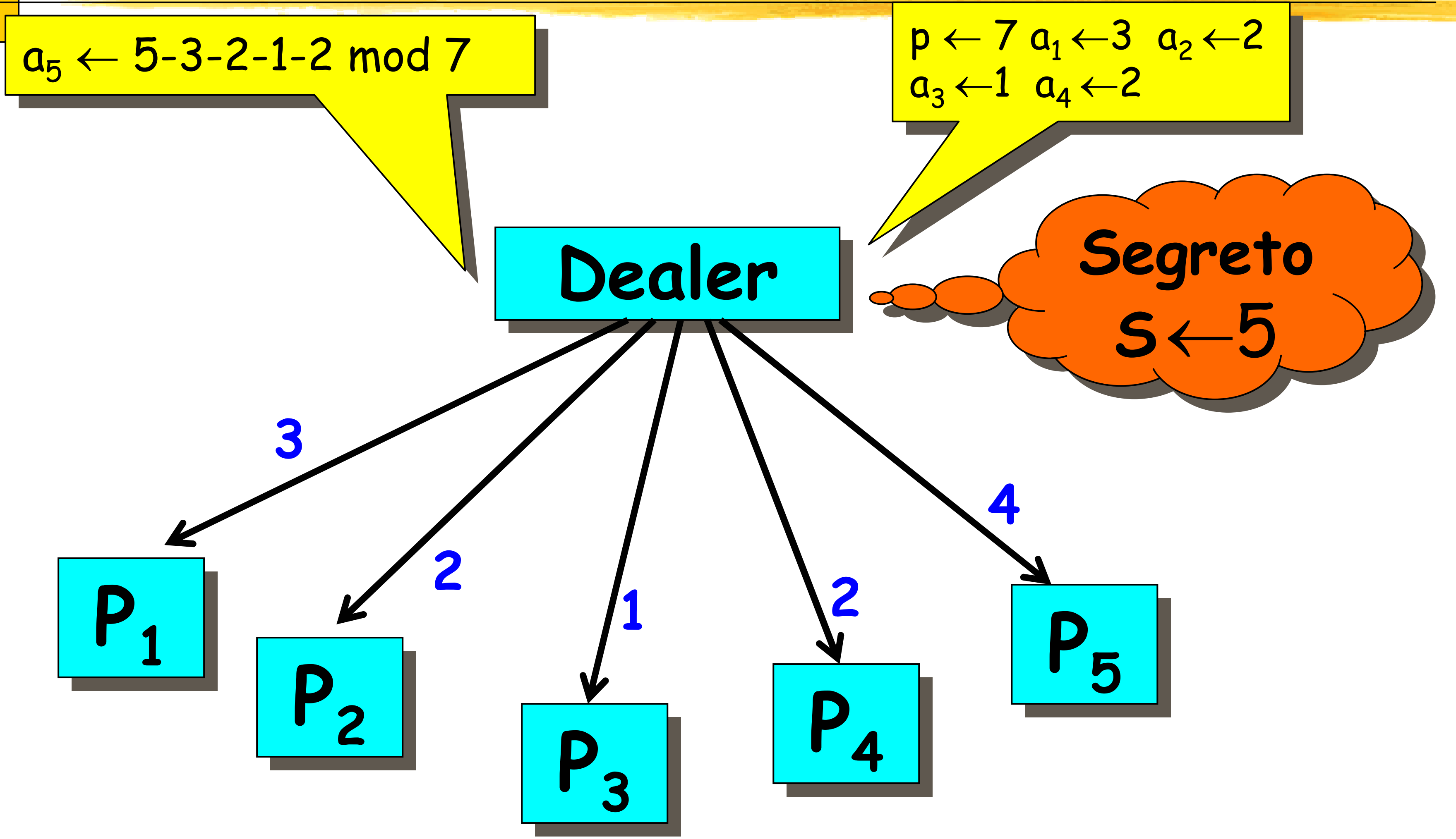
Calcolo share schema (n,n)



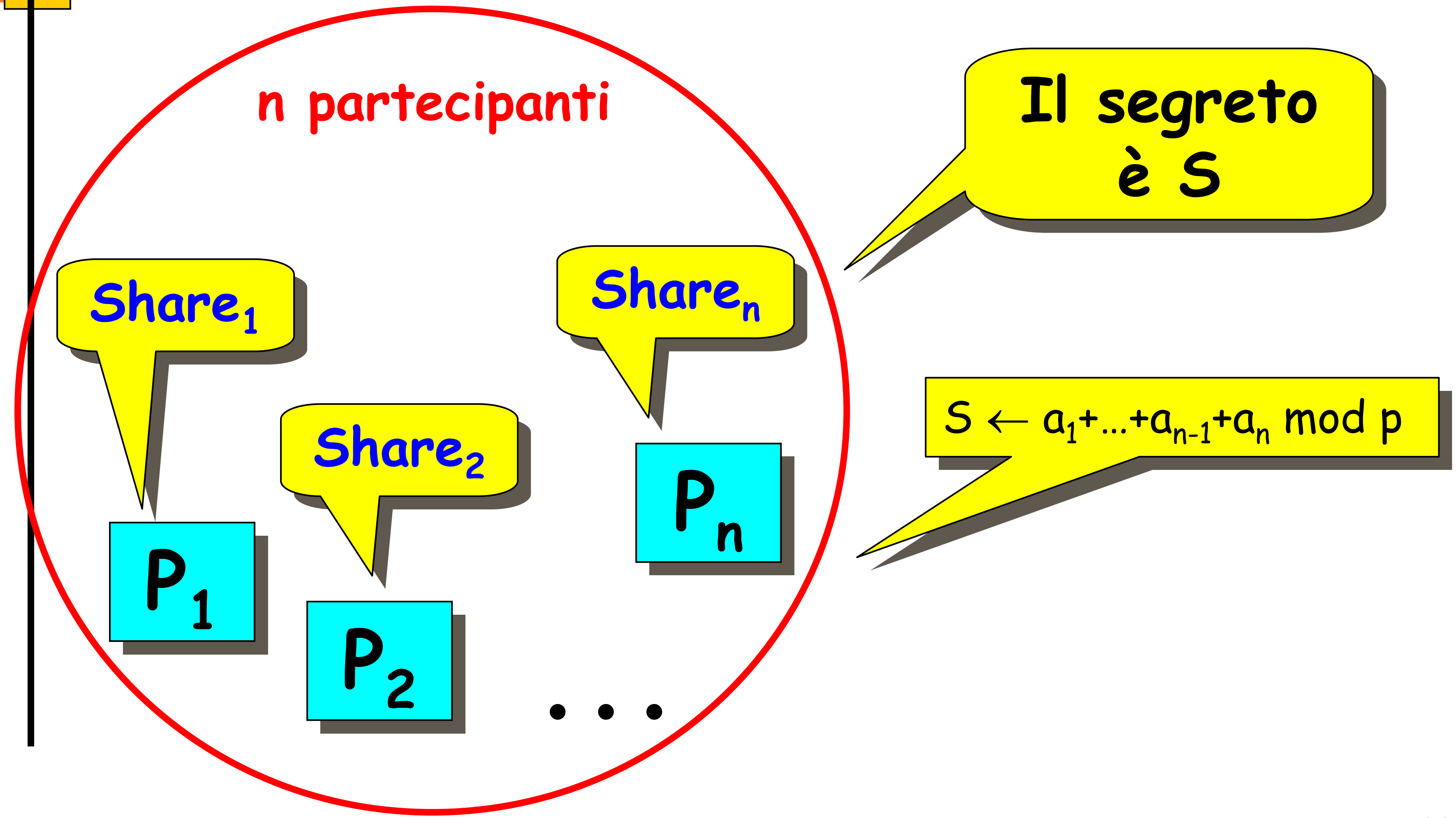
Distribuzione share



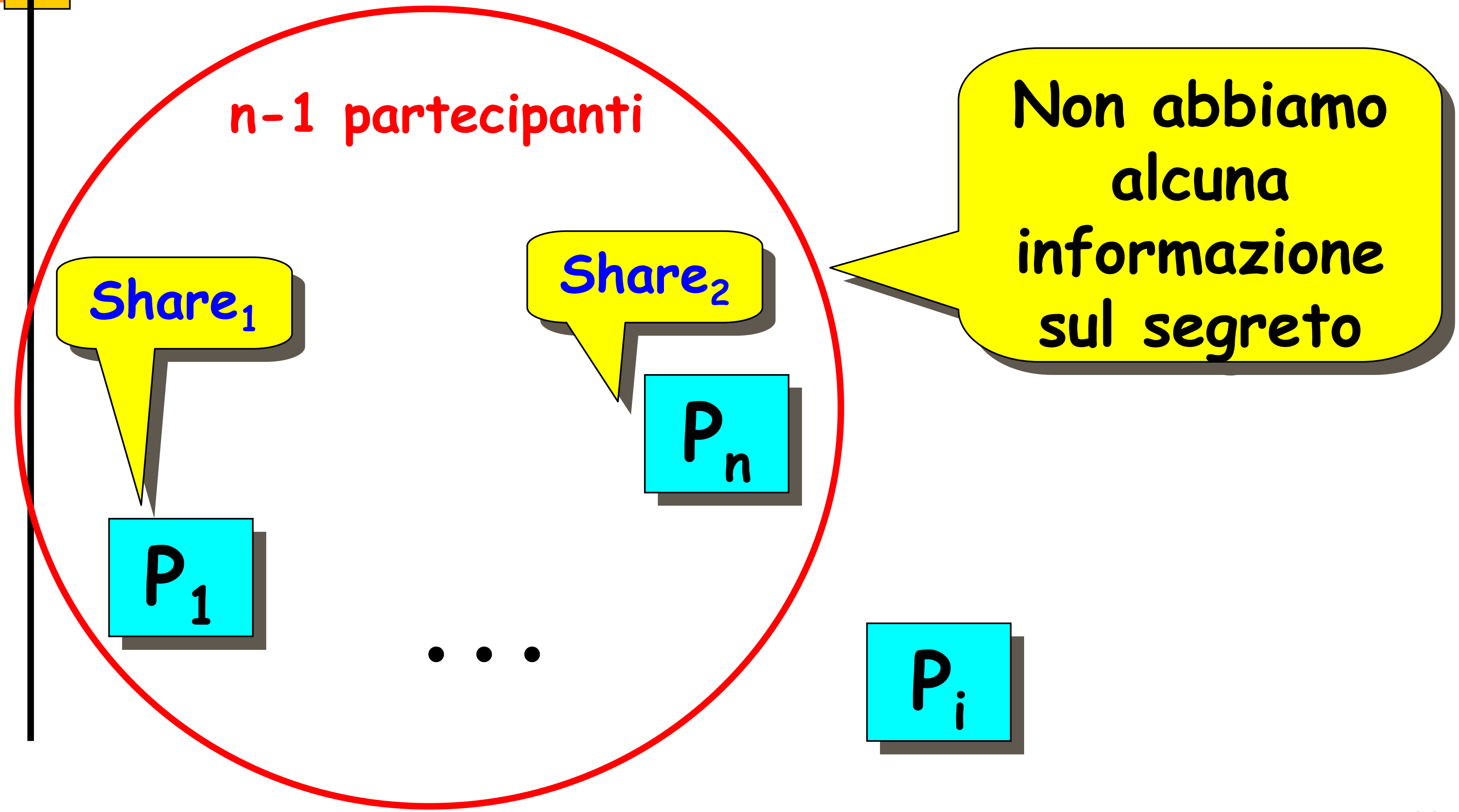
Esempio schema (5,5)



Ricostruzione del segreto



Ricostruzione del segreto



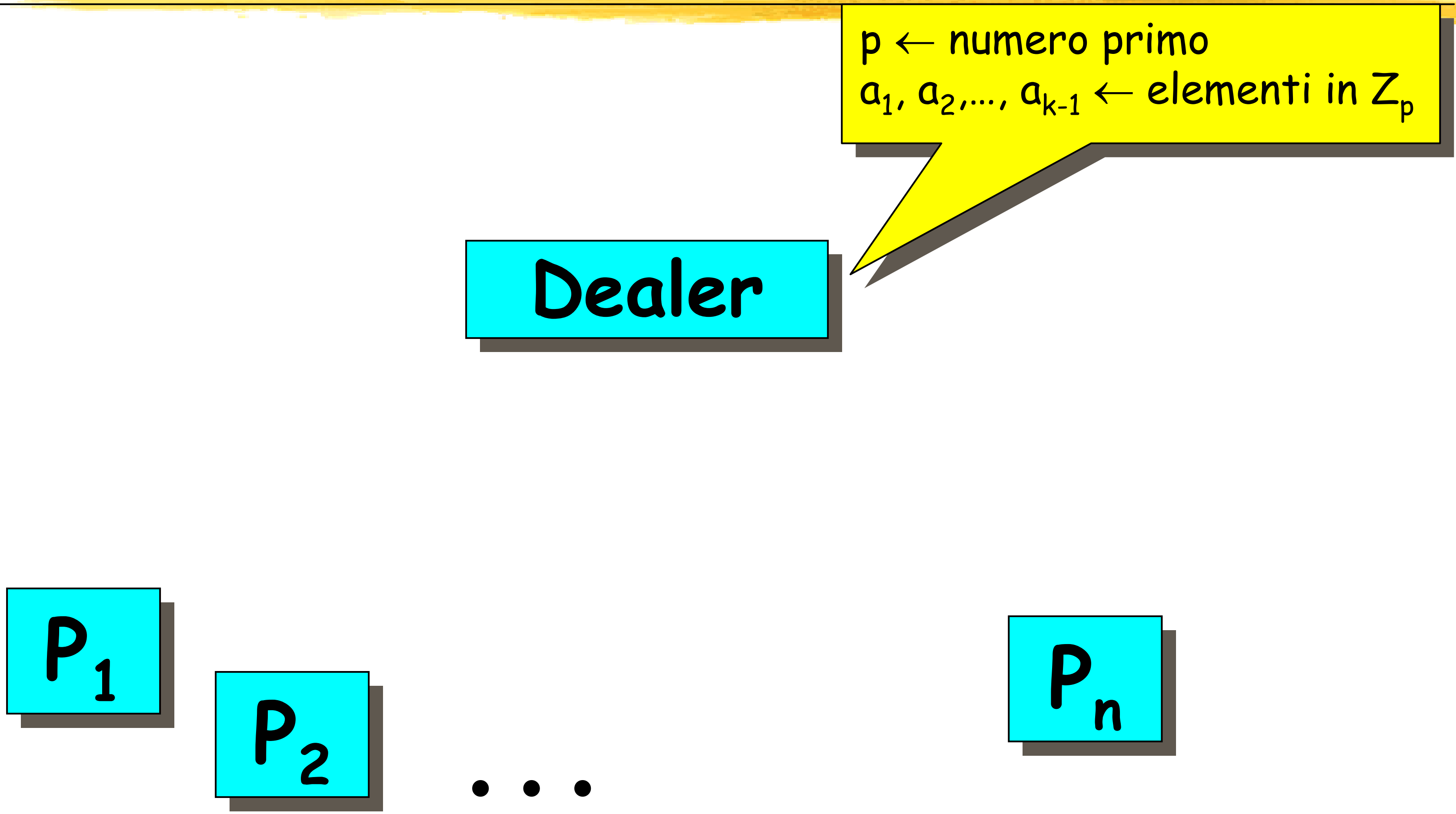
Esempio schema (5,5)

- P_1 sa che $3 = a_1$
- P_2 sa che $2 = a_2$
- P_3 sa che $1 = a_3$
- P_5 sa che $4 = S\text{-}a_1\text{-}a_2\text{-}a_3\text{-}a_4 \bmod 7$

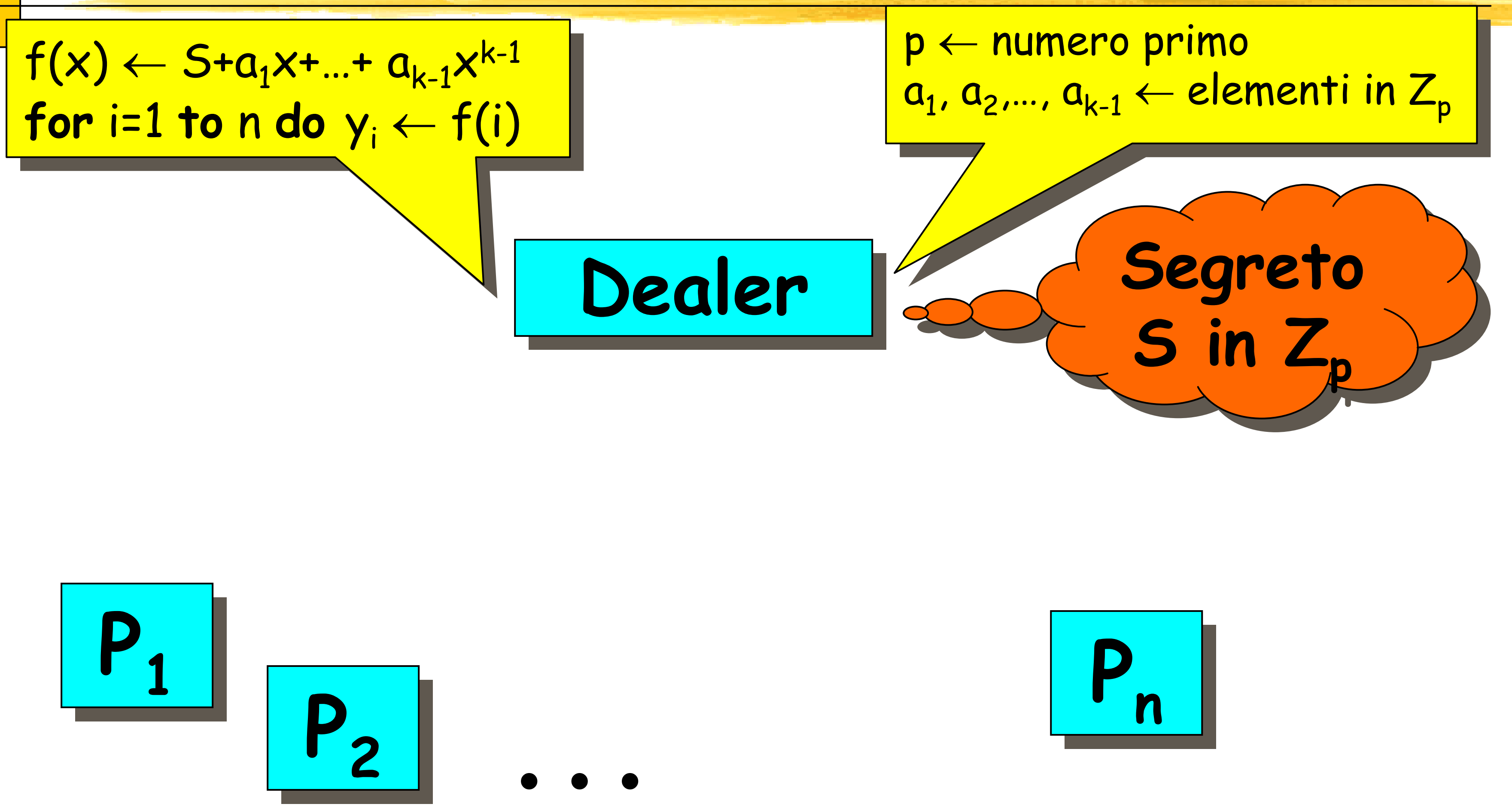
Il sistema ha 7 soluzioni:

S	a_4
0	4
1	5
2	6
3	0
4	1
5	2
6	3

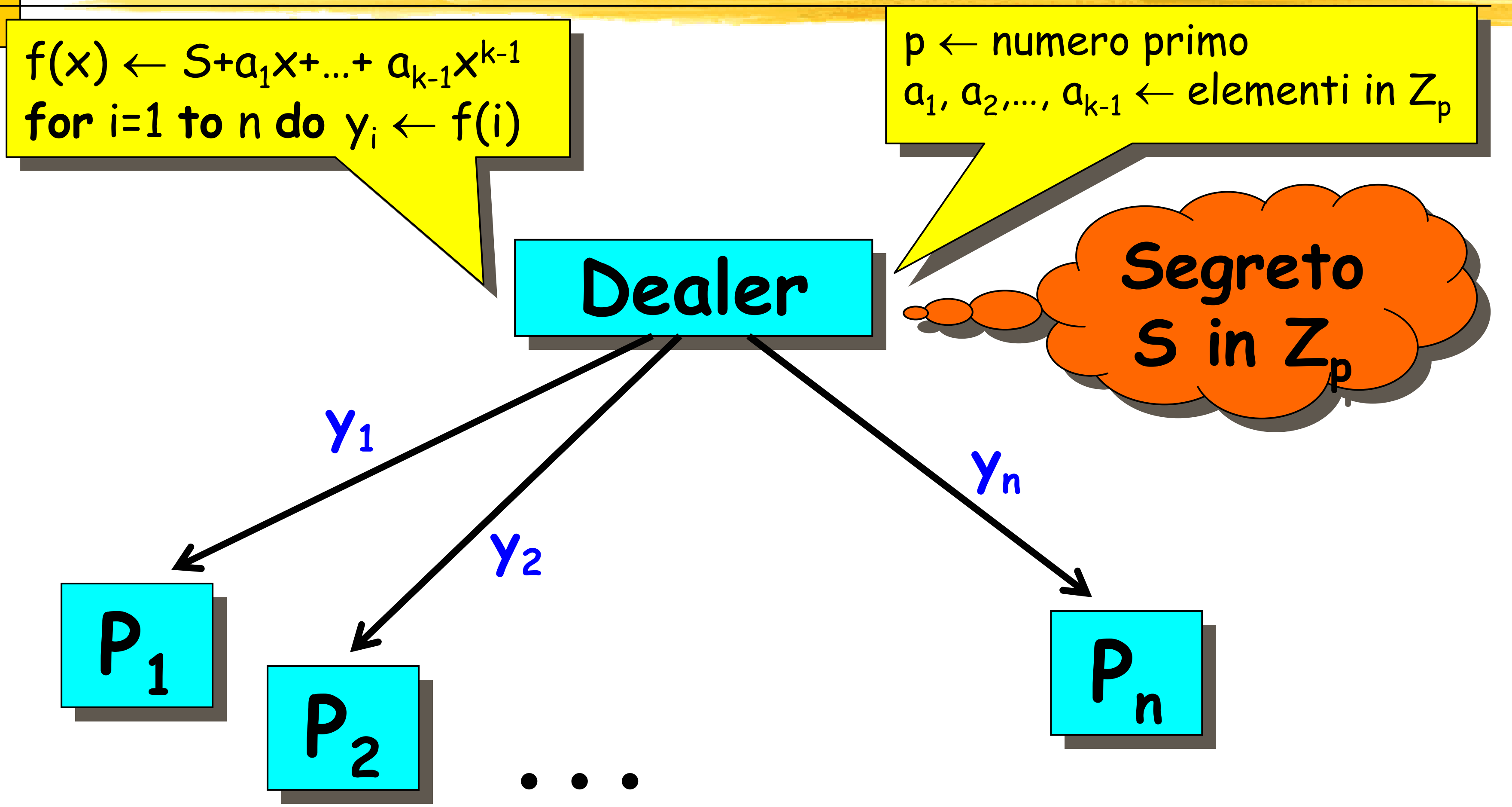
Inizializzazione schema (k,n)



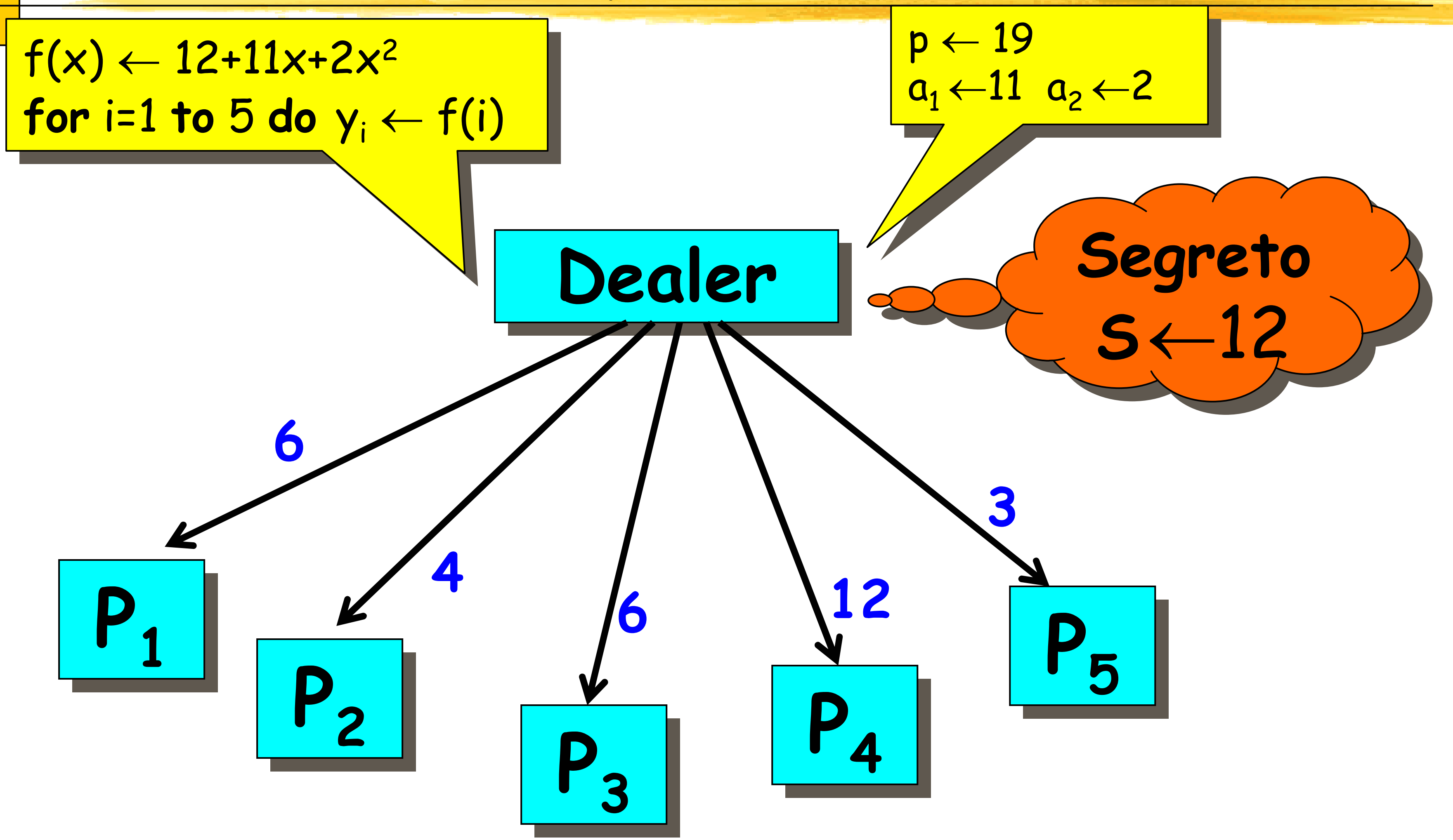
Calcolo share schema (k,n)



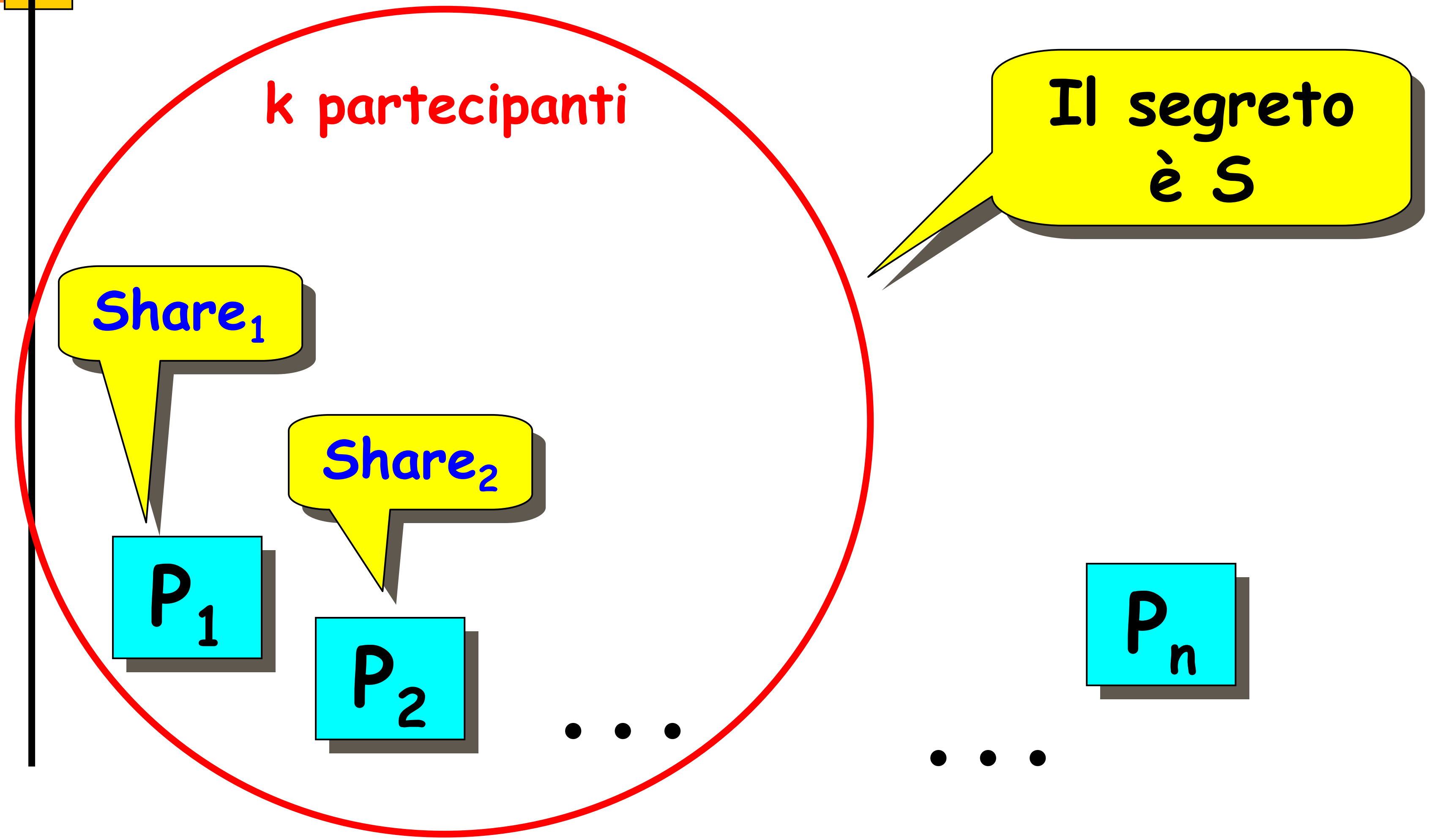
Distribuzione share



Esempio schema (3,5)



Ricostruzione del segreto



Informazioni k partecipanti

- k equazioni: $y_i = S+a_1 i+\ldots+ a_{k-1}i^{k-1}$ per $i=i_1, i_2, \ldots i_k$
- k incognite: $S, a_1,\ldots, a_{k-1}$
- Possono ricostruire il segreto!

Esempio schema (3,5)

- P_1 sa che $6 = S + a_1 \cdot 1 + a_2 \cdot 1^2$
- P_2 sa che $4 = S + a_1 \cdot 2 + a_2 \cdot 2^2$
- P_4 sa che $12 = S + a_1 \cdot 4 + a_2 \cdot 4^2$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 4 & 16 \end{bmatrix} \begin{bmatrix} S \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \\ 12 \end{bmatrix}$$

det = (2-1)(4-1)(4-2) mod 19
= 6

Il sistema ha un'unica soluzione:

$S=19 \quad a_1 = 11 \quad a_2 = 2$

Informazioni k partecipanti

Partecipanti $P_{i_1}, P_{i_2}, \ldots, P_{i_k}$

$$\begin{bmatrix} 1 & i_1 & i_1^{\,2} & \cdots & i_1^{\,k-1} \\ 1 & i_2 & i_2^{\,2} & \cdots & i_2^{\,k-1} \\ 1 & i_3 & i_3^{\,2} & \cdots & i_3^{\,k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & i_k & i_k^{\,2} & \cdots & i_k^{\,k-1} \end{bmatrix} \begin{bmatrix} S \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{bmatrix} = \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ y_{i_3} \\ \vdots \\ y_{i_k} \end{bmatrix}$$

Matrice di Vandermonde $\det = \prod_{1 \le r < t \le k} (i_t - i_r) \bmod p$

Il sistema ha un'unica soluzione

Calcolo del Segreto

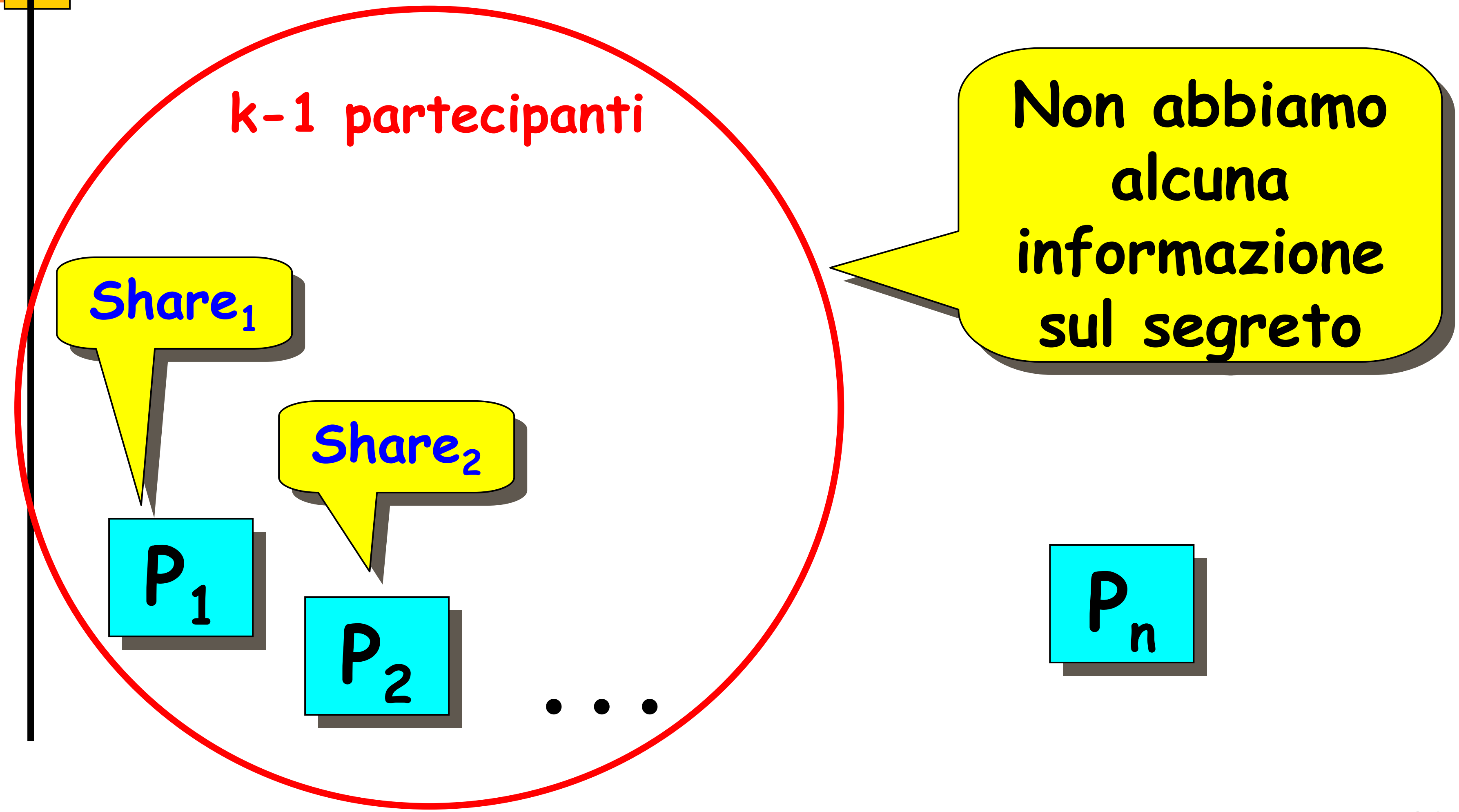
- Calcolo polinomio f(x)
- Formula di interpolazione di Lagrange
  - Grado k-1
  - $f(i_j) = y_{i_j}$

$$f(x) = \sum_{j=1}^{k} y_{i_j} \prod_{\substack{1 \le t \le k \\ t \ne j}} \frac{x - i_t}{i_j - i_t}$$

- Serve solo $f(0) = S$

$$f(0) = \sum_{j=1}^{k} y_{i_j} \prod_{\substack{1 \le t \le k \\ t \ne j}} \frac{i_t}{i_t - i_j}$$

Ricostruzione del segreto



Informazioni k-1 partecipanti

- k-1 equazioni: $y_i = S+a_1 i+\ldots+ a_{k-1} i^{k-1}$ per $i=i_1, i_2, \ldots i_{k-1}$
- k incognite: $S, a_1,\ldots, a_{k-1}$
- Non possono ricostruire il segreto
- Ogni segreto è equamente possibile

Esempio schema (3,5)

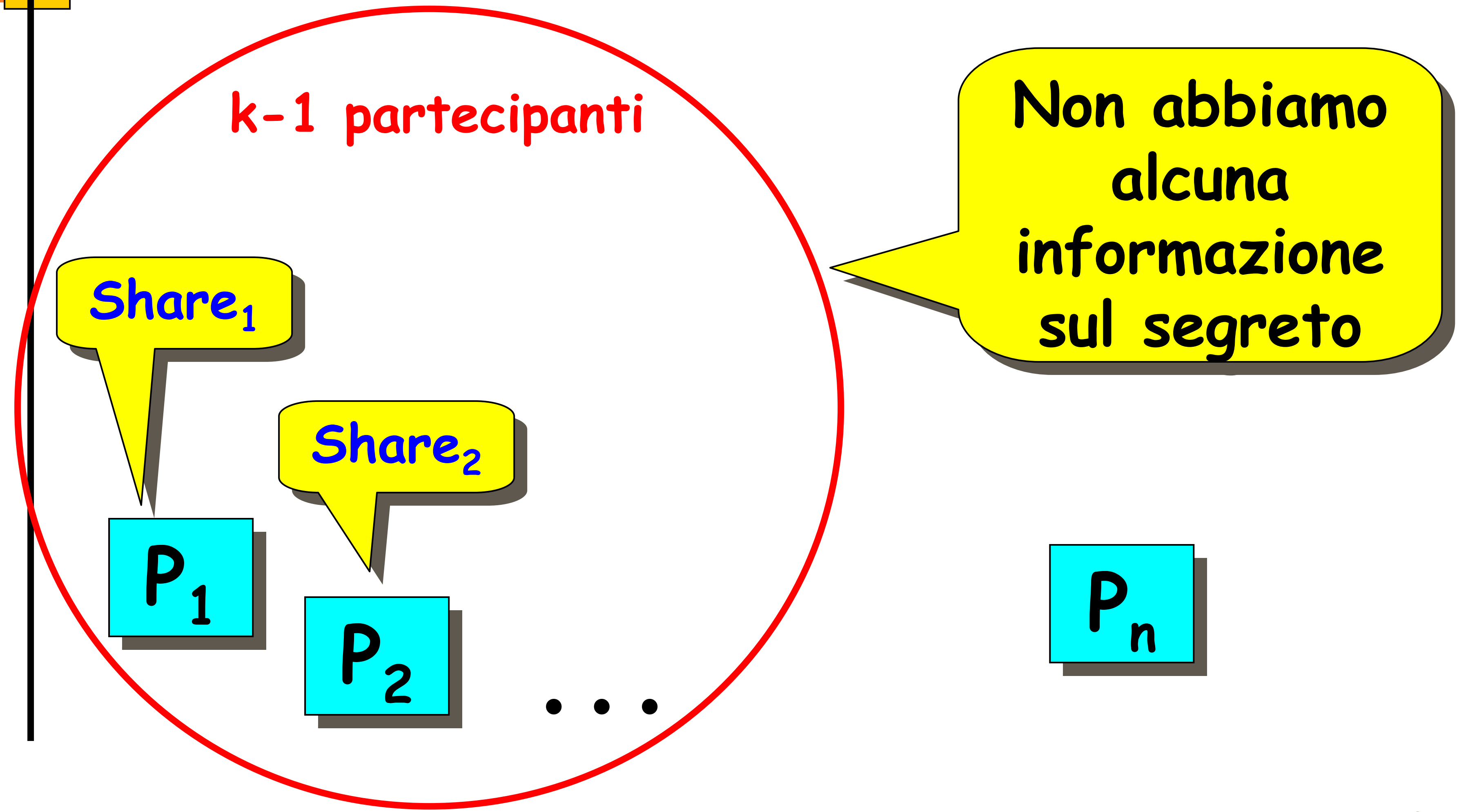
- P_1 sa che $6 = S + a_1 \cdot 1 + a_2 \cdot 1^2$
- P_2 sa che $4 = S + a_1 \cdot 2 + a_2 \cdot 2^2$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} S \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} 6 \\ 4 \end{bmatrix}$$

Il sistema ha 19 soluzioni:

S	a_1	a_2
0	10	15
1	18	6
2	7	16
3	15	7
4	4	17
5	12	8
6	1	18
7	9	9
8	17	0
9	6	10
10	14	20
11	3	11
12	11	2
13	0	12
14	8	3
15	16	13
16	5	4
17	13	14
18	2	5

Ricostruzione del segreto



Informazioni
k-1 partecipanti

- k-1 equazioni: $y_i = S+a_1 i+\ldots+ a_{k-1} i^{k-1}$ per $i=i_1, i_2, \ldots i_{k-1}$
- k incognite: $S, a_1,\ldots, a_{k-1}$
- Ipotizzando un valore per il segreto S

$$y_{i_k} = F(i_k) = S+a_1 0+\ldots+ a_{k-1} 0^{k-1}$$

$$\begin{bmatrix} 1 & i_1 & {i_1}^2 & \cdots & {i_1}^{k-1} \\ 1 & i_2 & {i_2}^2 & \cdots & {i_2}^{k-1} \\ 1 & i_3 & {i_3}^2 & \cdots & {i_3}^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & i_k & {i_k}^2 & \cdots & {i_k}^{k-1} \end{bmatrix} \begin{bmatrix} S \\ a_1 \\ a_2 \\ \vdots \\ a_{k-1} \end{bmatrix} = \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ y_{i_3} \\ \vdots \\ y_{i_k} \end{bmatrix}$$

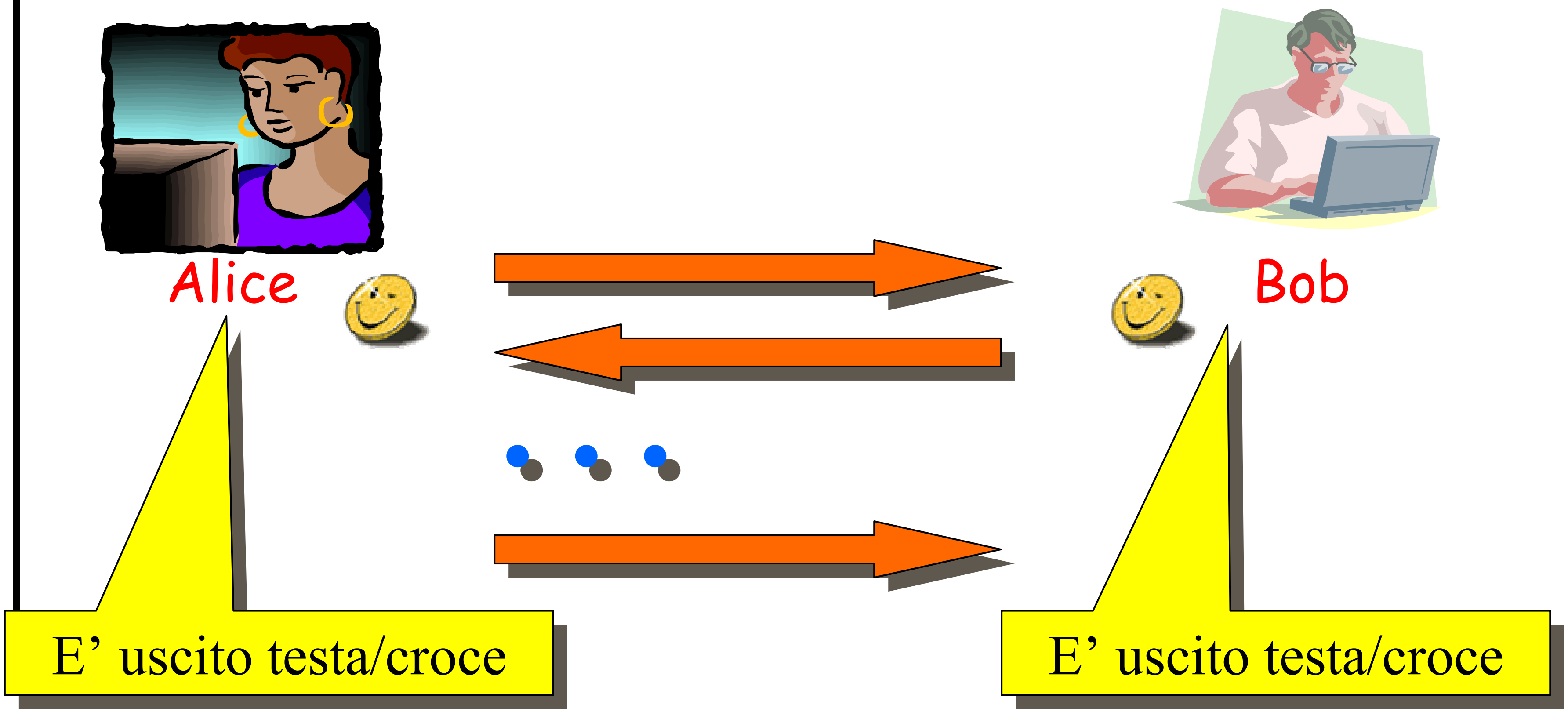
$$i_k = 0$$

$$\det = \prod_{1 \le r < t \le k} (i_t - i_r) \bmod p$$

Matrice di Vandermonde

Il sistema ha un'unica soluzione

Lancio di una moneta



Lancio di una moneta
protocollo *naive*

Alice

Bob

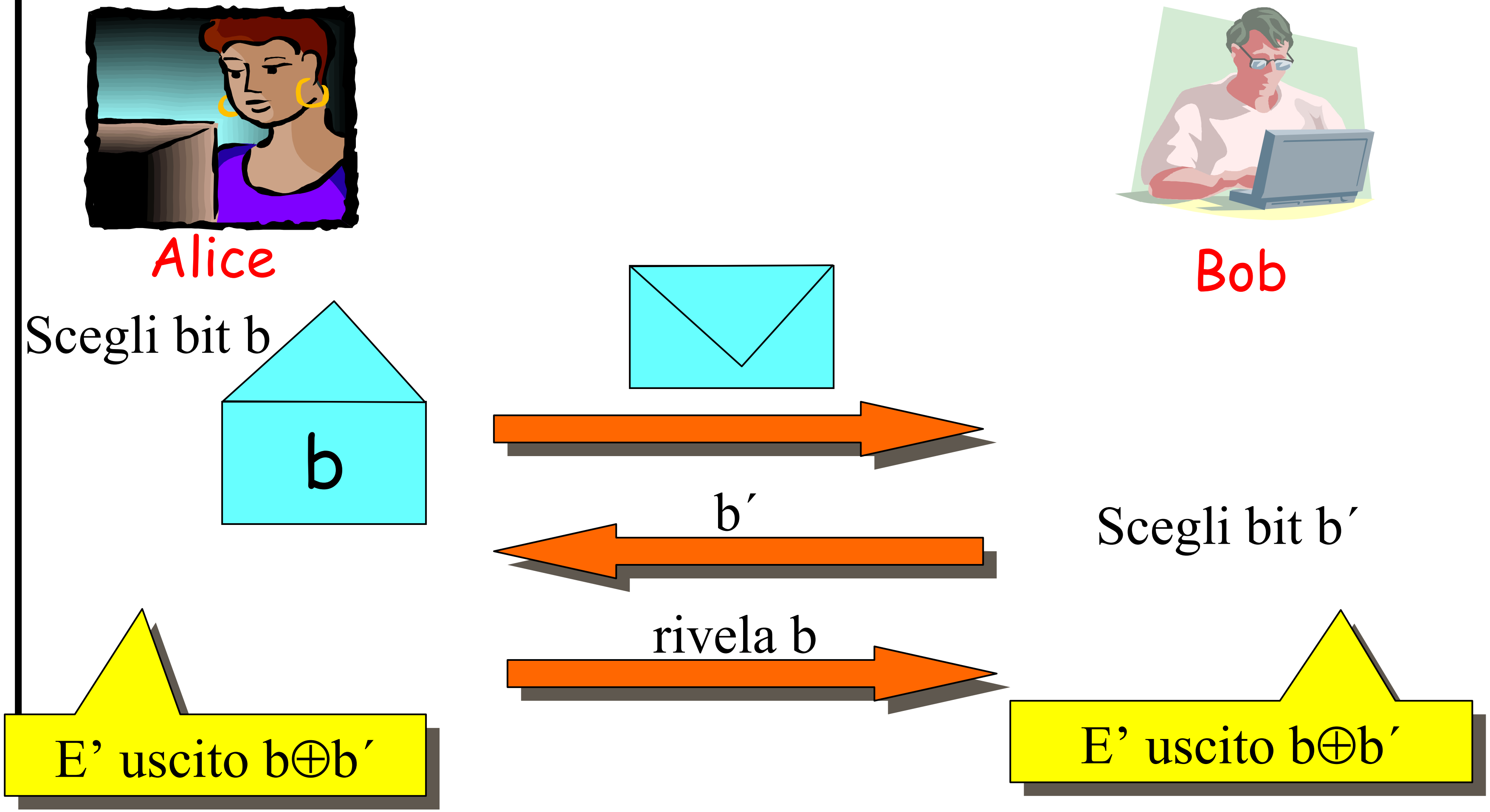
Lancio moneta

testa

E' uscito testa

E' uscito testa

Lancio di una moneta



Lancio di una moneta

Alice

Bob

Scegli bit b

x←commitment(b)

x →

← b´

Scegli bit b´

rivela b →

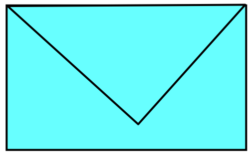
E’ uscito b⊕b´

E’ uscito b⊕b´

Commitment

x←commitment(b)

Equivalente digitale di una busta



- "Facile" da calcolare
- Dato x è "difficile" calcolare b
- "Facile" mostrare che x = commitment(b)
- "Difficile" mostrare che x = commitment(1-b)

Commitment

$x \leftarrow commitment(b)$

b = predicato_difficile (x)

Esempio

$C = M^e \bmod n$

$parità_{n,e}(C)$ = bit meno significativo di M

$$half_{n,e}(C) = \begin{cases} 0 & \text{se } M < n/2 \\ 1 & \text{se } M > n/2 \end{cases}$$

Blind Signature

Voglio avere la firma di M da parte di B

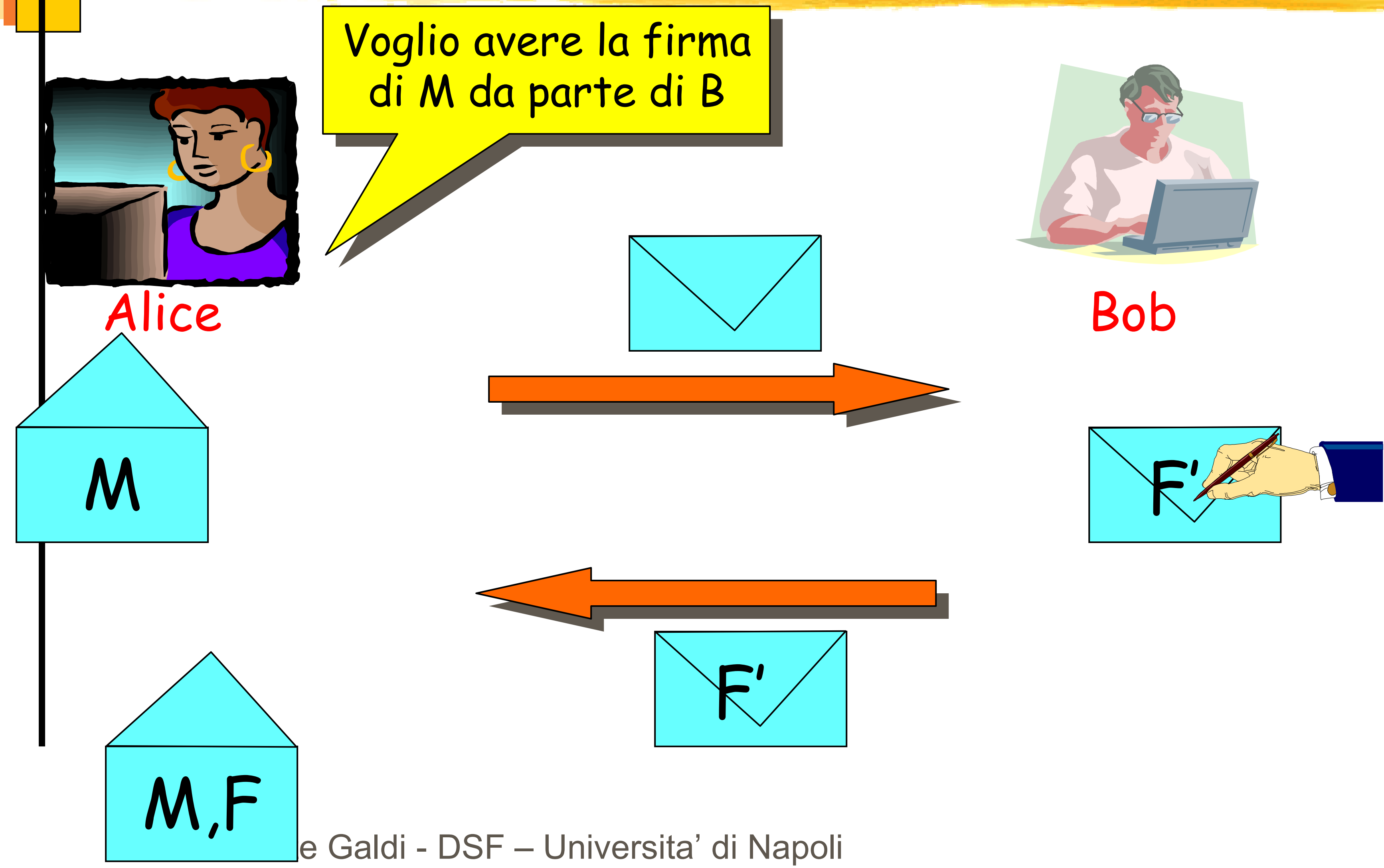
Alice

Bob

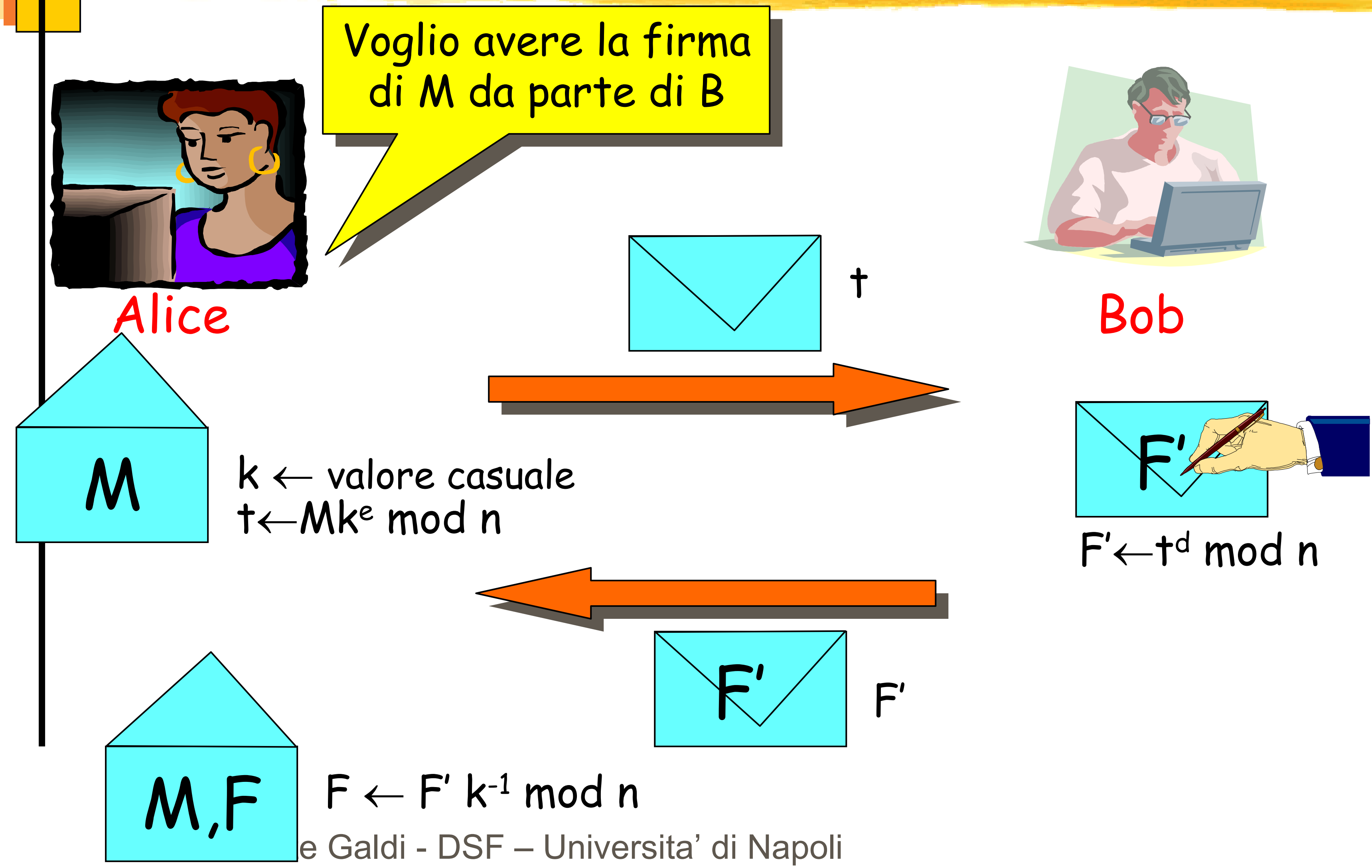
F è la firma di M da parte di B

Non so che cosa ho firmato

Blind Signature
protocollo con busta



Blind Signature
protocollo con RSA



Blind Signature
protocollo con RSA

Voglio avere la firma di M da parte di B

Alice

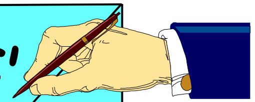
Bob

t

M

k ← valore casuale

$t \leftarrow Mk^e \bmod n$



F'

$F' \leftarrow t^d \bmod n$

F'

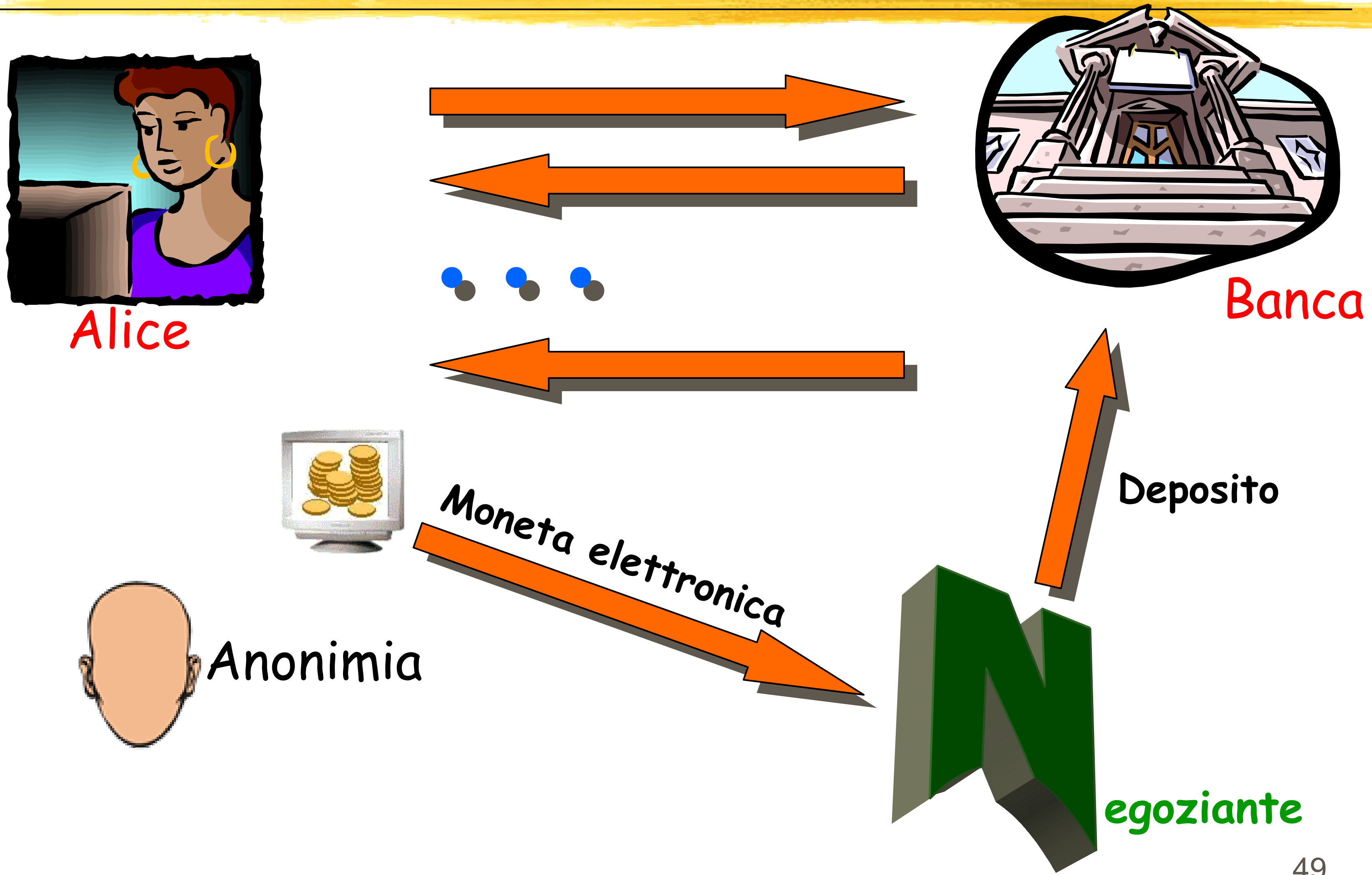
F'

$$
\begin{aligned}
F &= F'\, k^{-1} \bmod n \\
&= t^d\, k^{-1} \bmod n \\
&= (Mk^e)^d\, k^{-1} \bmod n \\
&= M^d\, k^{ed}\, k^{-1} \bmod n \\
&= M^d \bmod n
\end{aligned}
$$

M,F

$F \leftarrow F'\, k^{-1} \bmod n$

Moneta Elettronica

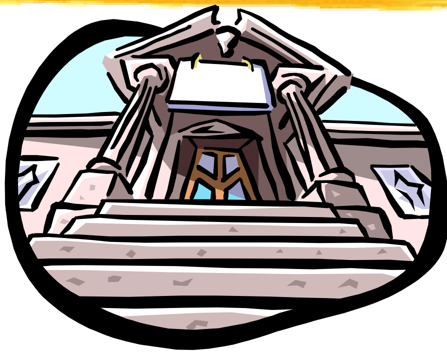


Moneta Elettronica 0

Alice

Assegno \$1000

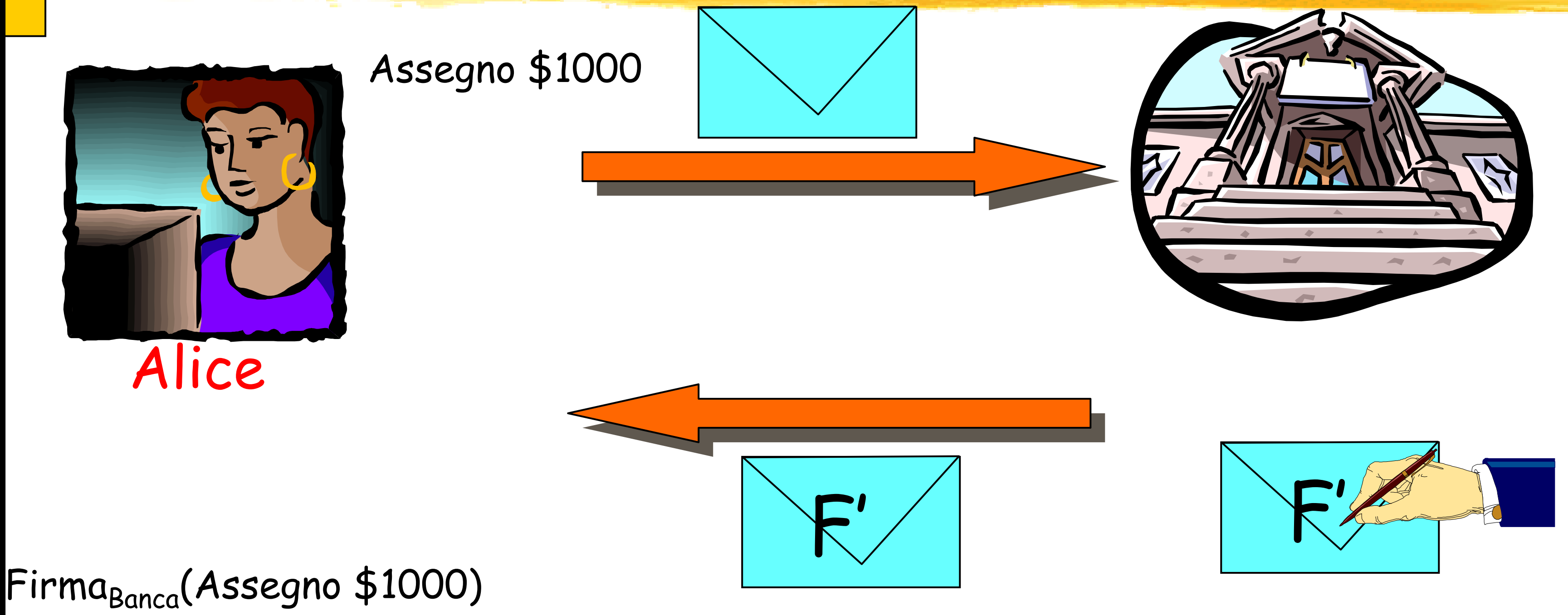
Firma$_{Banca}$(Assegno \$1000)



- La banca puo' memorizzare "importo-firma"

Problemi?

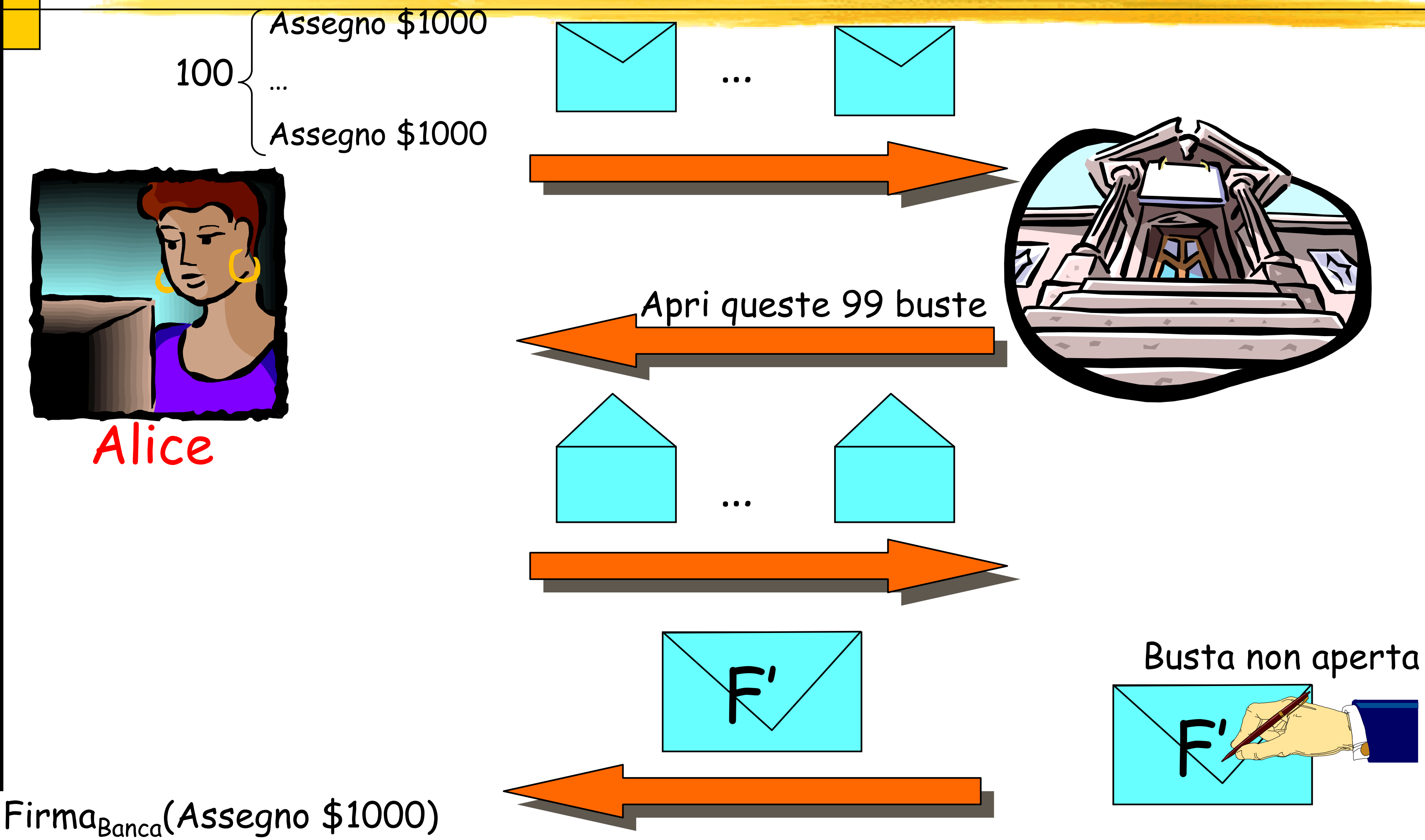
Moneta Elettronica I



Assegno di $1000?

Problemi?

Moneta Elettronica II

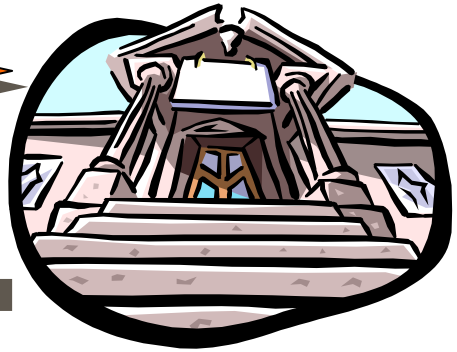


Moneta Elettronica II

100 { Assegno \$1000 … Assegno \$1000 }

…


Alice



Apri queste 99 buste

…

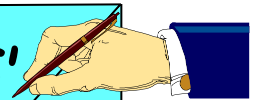
Problemi?

Alice puo' spendere l'assegno piu' volte!!!

F'

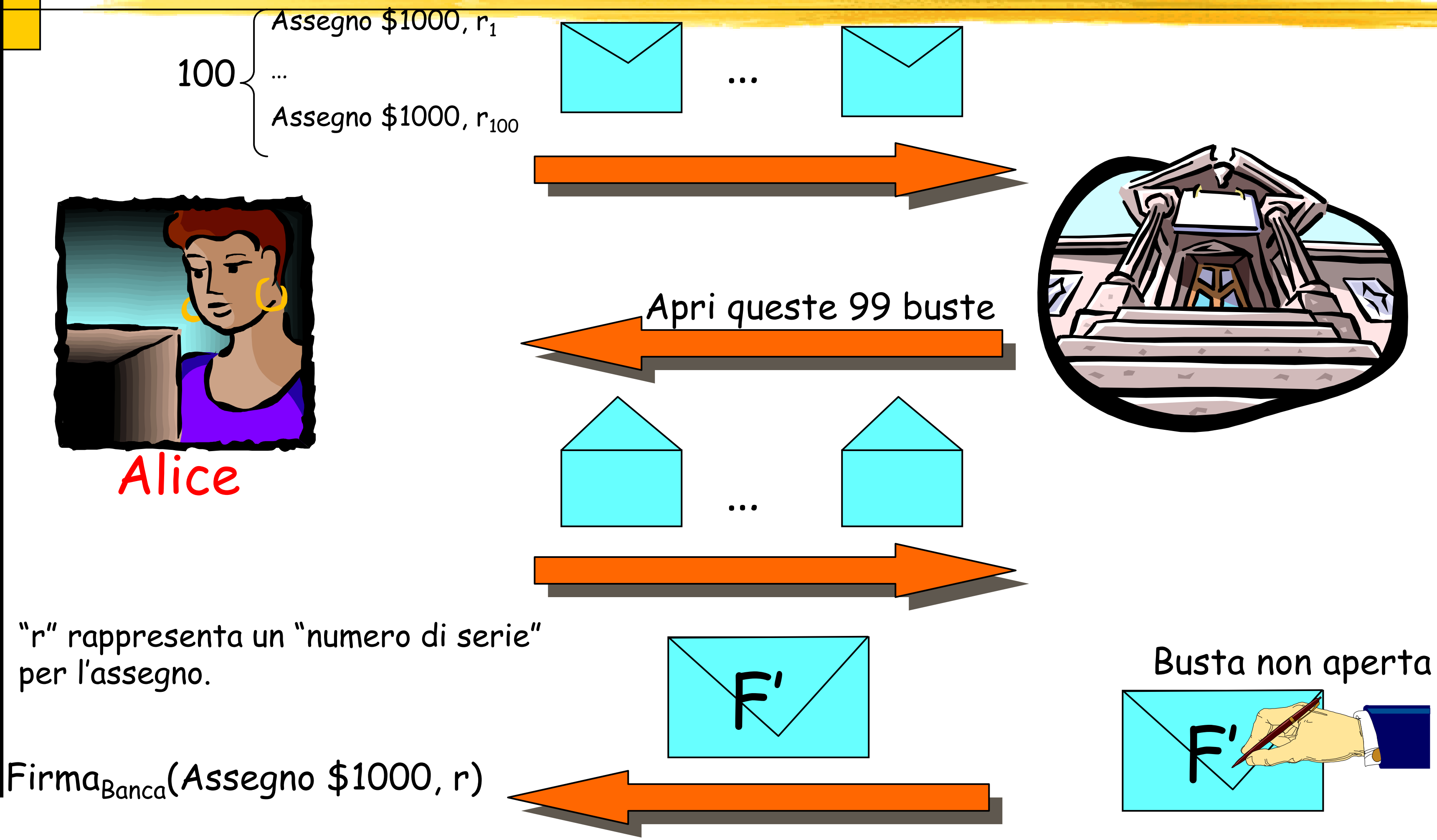
Busta non aperta

F'



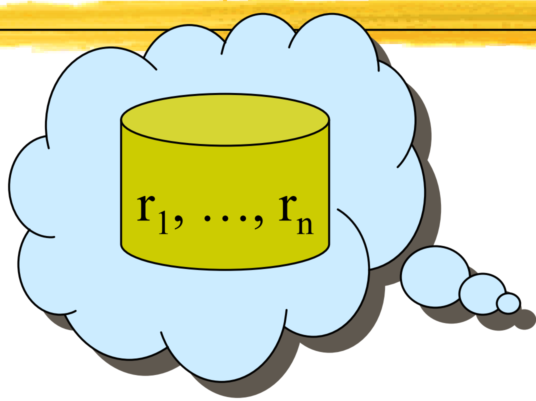
$Firma_{Banca}$(Assegno \$1000)

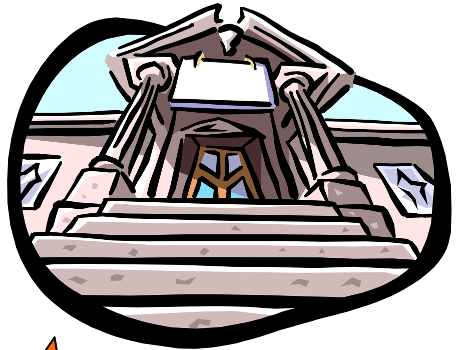
Moneta Elettronica III



Moneta Elettronica III

Alice





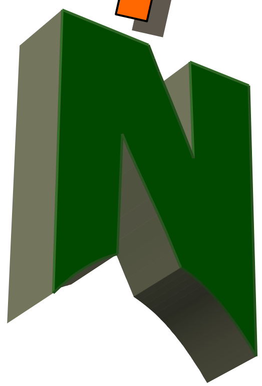
$\text{Firma}_{\text{Banca}}(\text{Assegno } \$1000, r)$

Deposito

$\text{Firma}_{\text{Banca}}(\text{Assegno } \$1000, r)$

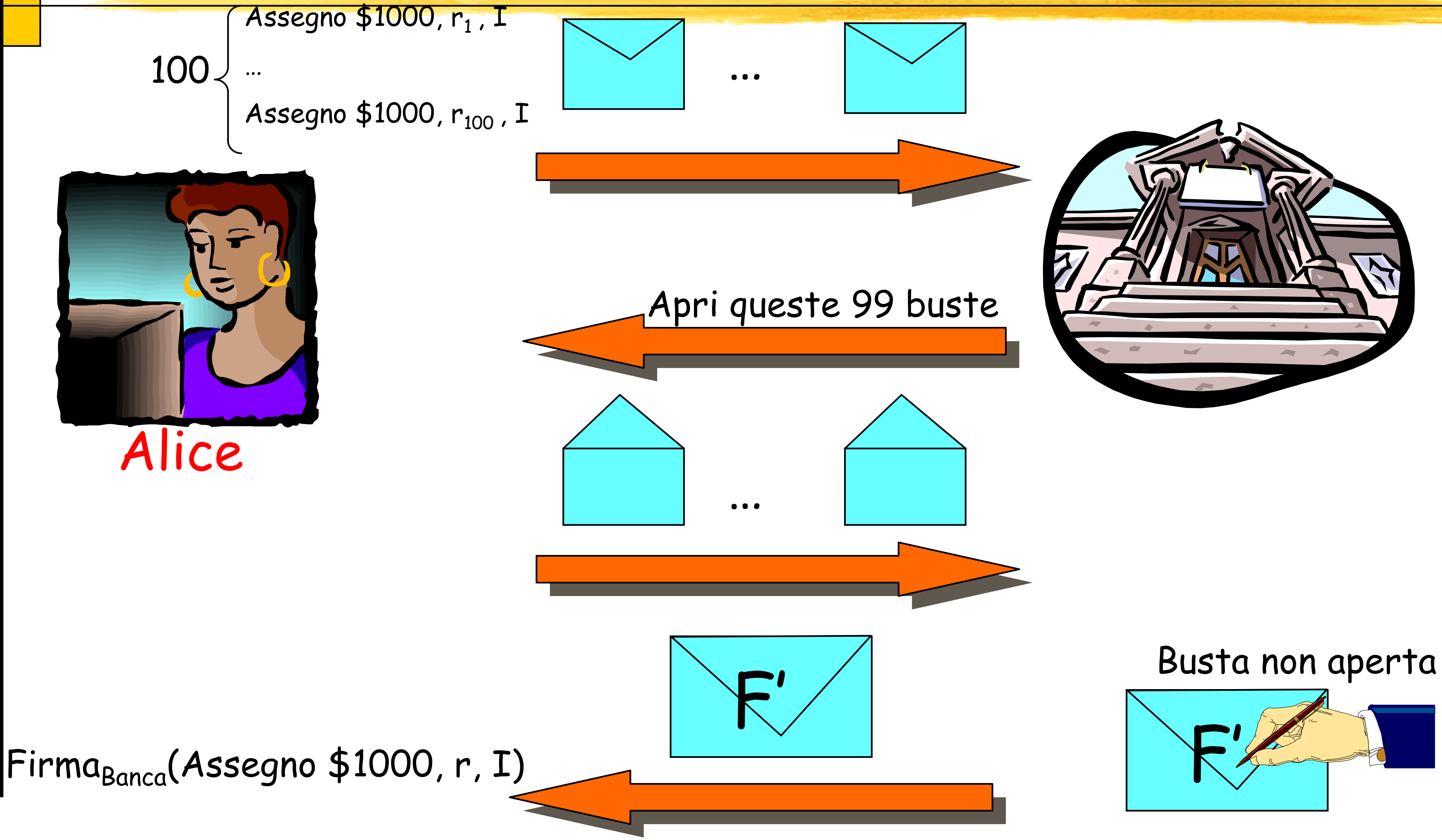
Problemi?

La banca puo' identificare un assegno speso piu' volte... Ma non puo' identificare il truffatore
Il cliente o il negoziante ?



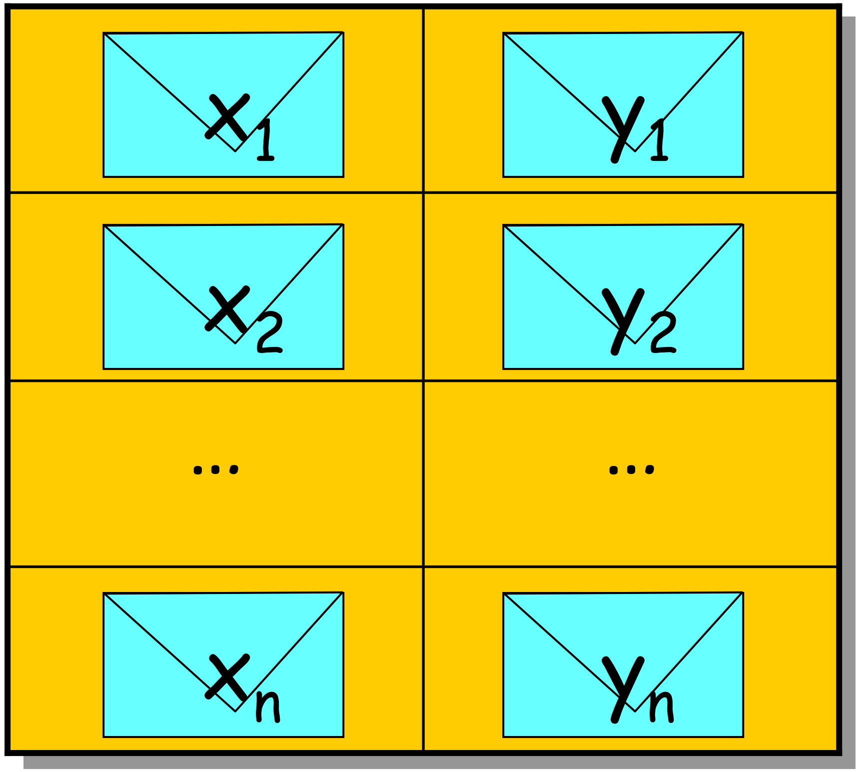
egoziante

Moneta Elettronica IV



Moneta Elettronica IV

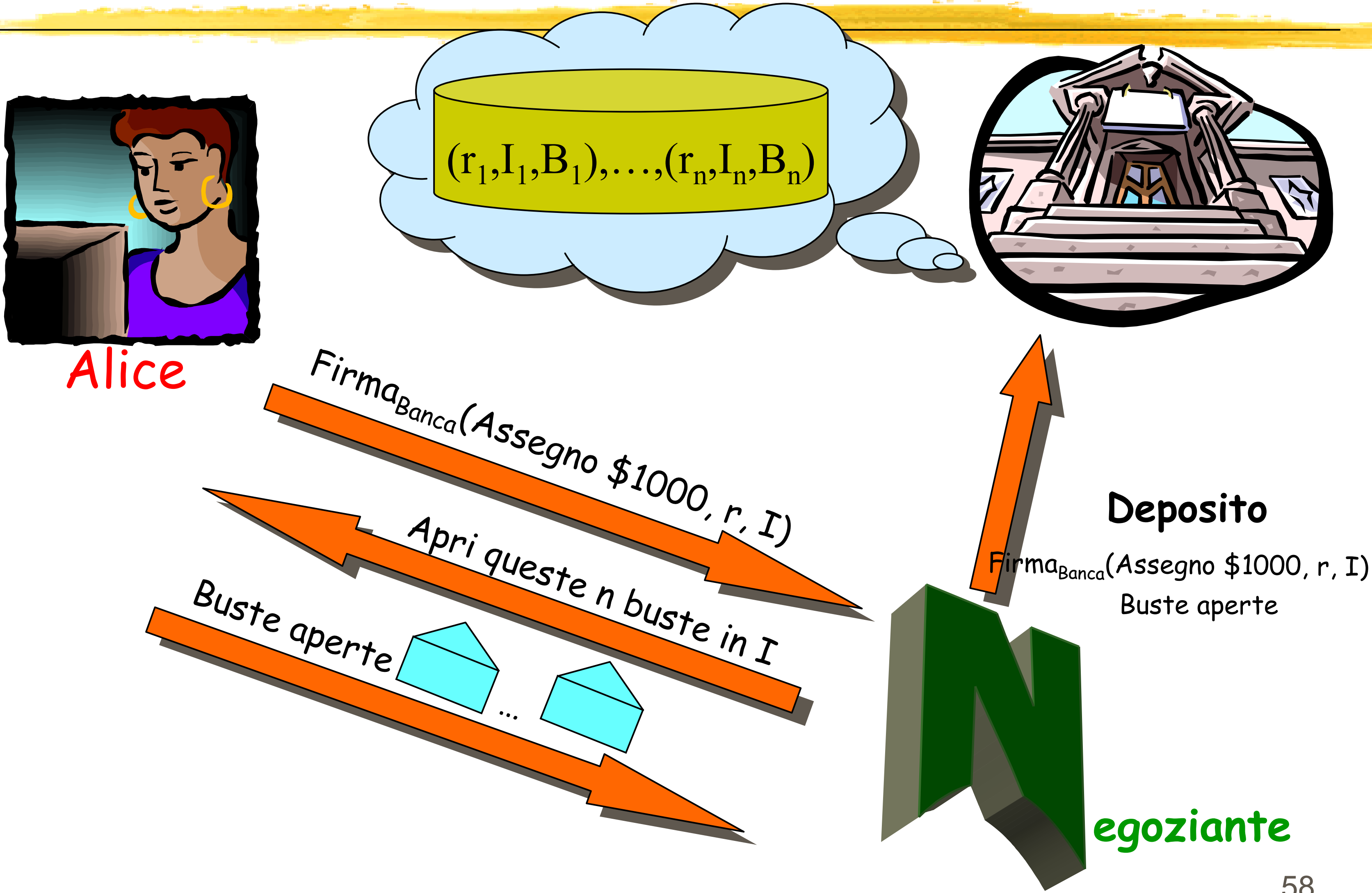
I



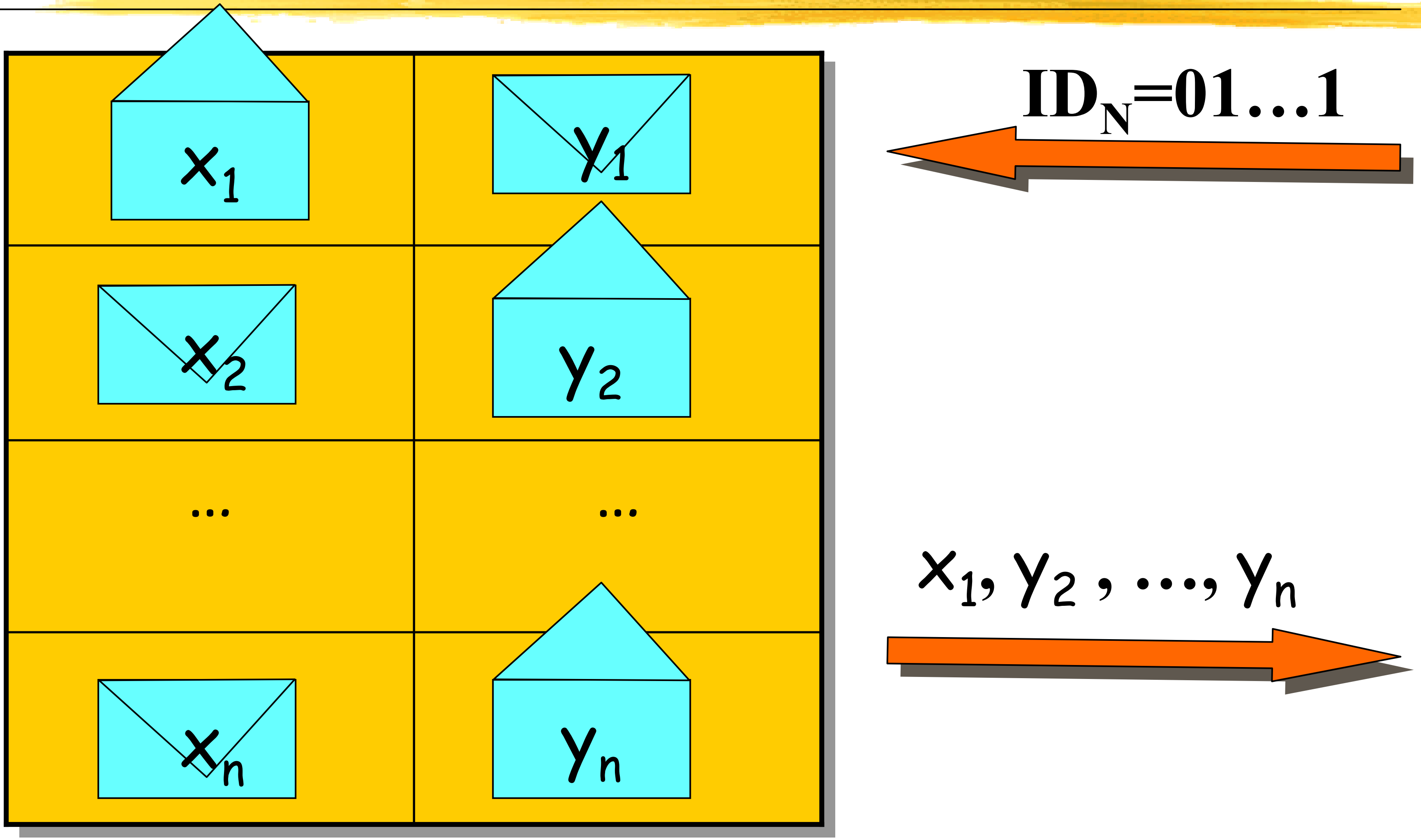
$x_i \oplus y_i = ID_{Alice}$

Condivisione segreti (2,2)

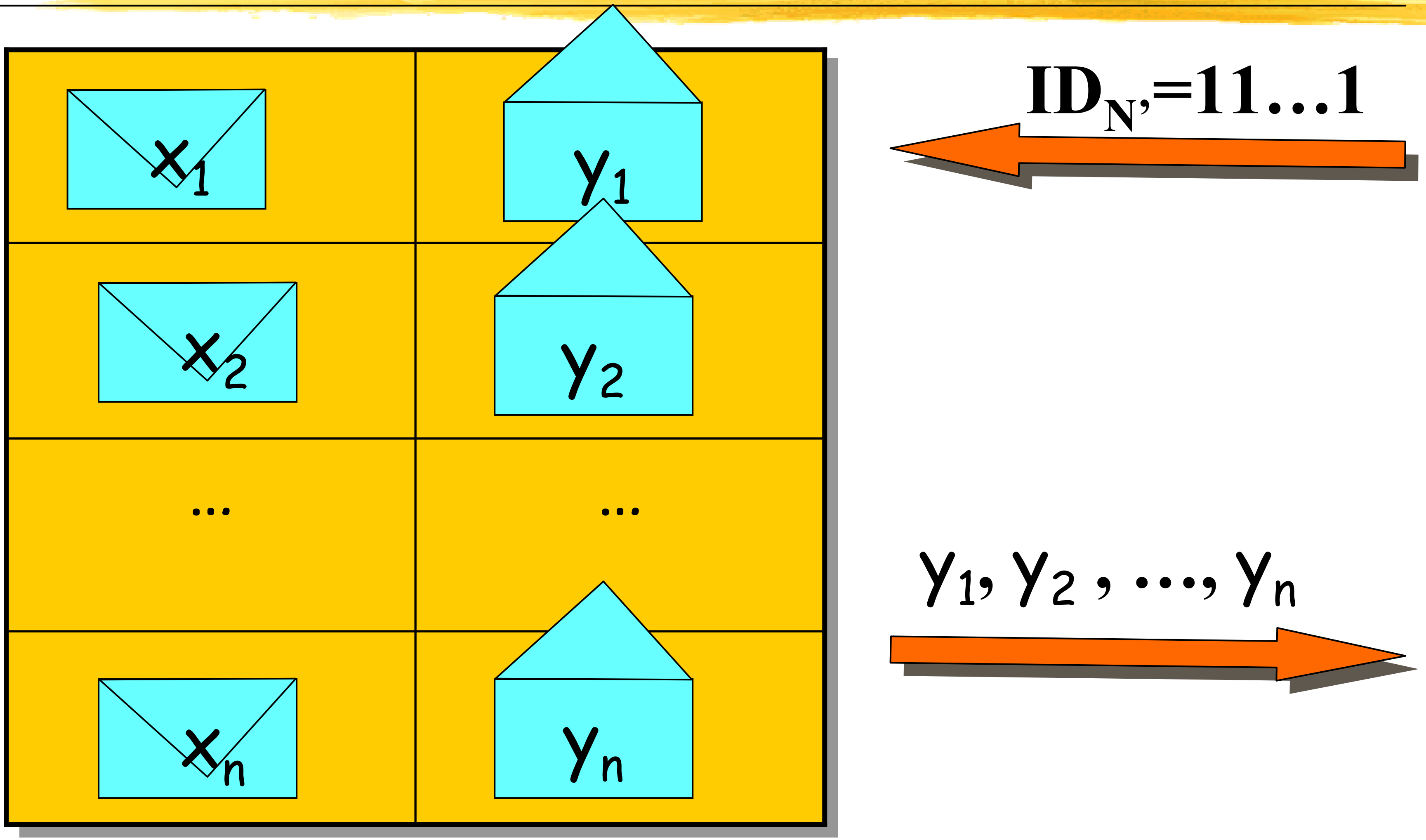
Moneta Elettronica IV



Moneta Elettronica IV

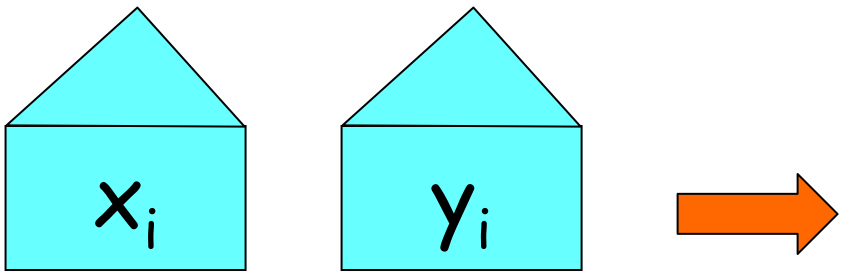


Moneta Elettronica IV



Moneta Elettronica IV

Se la moneta viene spesa due volte da Alice la banca scopre ID_{Alice}



$$x_i \oplus y_i = ID_{Alice}$$

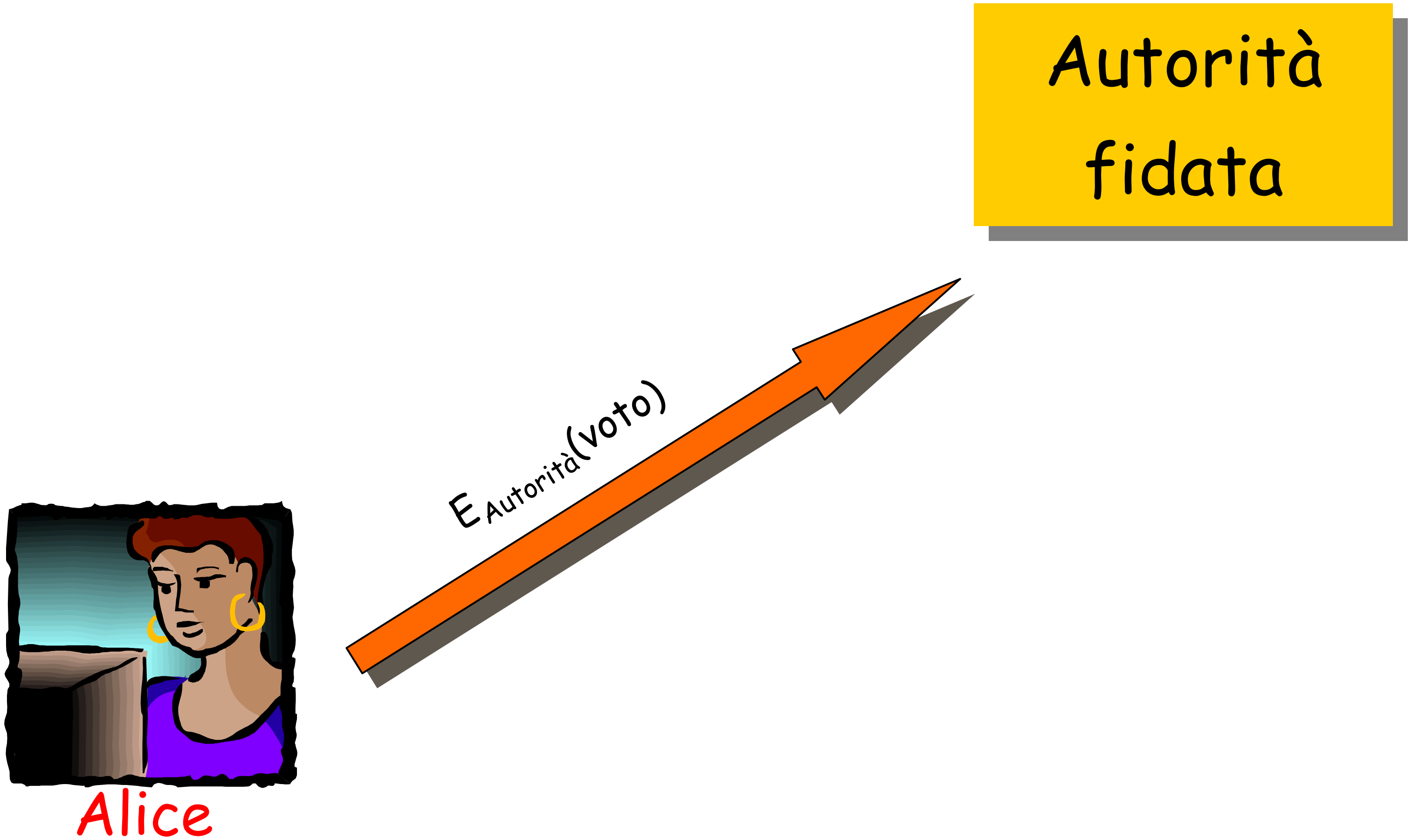
Moneta Elettronica IV

Commitment(x_1)	Commitment(y_1)
Commitment(x_2)	Commitment(Y_2)
…	…
Commitment(x_n)	Commitment(y_n)

Elezioni: proprietà

- Solo i votanti autorizzati possono votare
- Nessuno può votare più di una volta
- Voto anonimo
- Non si può duplicare il voto di un altro
- Non si può cambiare il voto di altri
- Ognuno può verificare che il proprio voto è conteggiato

Elezioni I: protocollo naive



Elezioni I: protocollo naive

Autorità fidata

$E_{\text{Autorità}}(\text{voto})$

Alice

Problemi?

Votanti autorizzati?

Più voti di un votante?

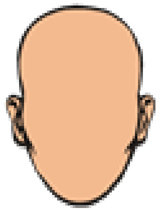
Elezioni II: protocollo naive

Autorità fidata

$E_{Autorità}(Firma_{Alice}(voto))$

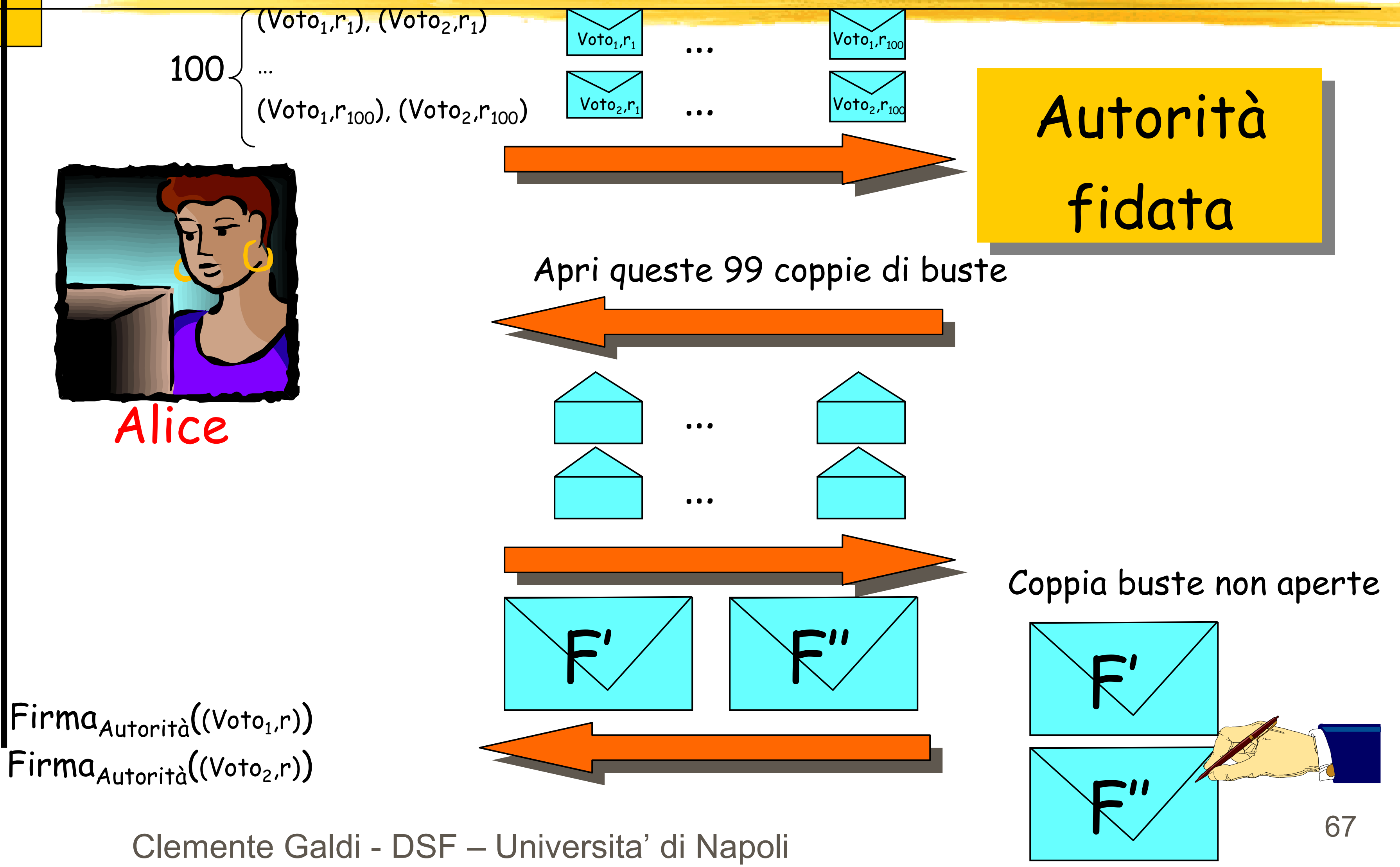
Alice

Problemi?



Anonimia

Elezioni III



Elezioni III

$r_1, \ldots, r_n$

Autorità fidata

Corretto!

Se l'Autorita' e' FIDATA!

$E_{Autorità}(Firma_{Autorità}((Voto_i, r)))$

Alice

Pubblicazione voti:

$Firma_{Autorità}((Voto_i, r))$

…

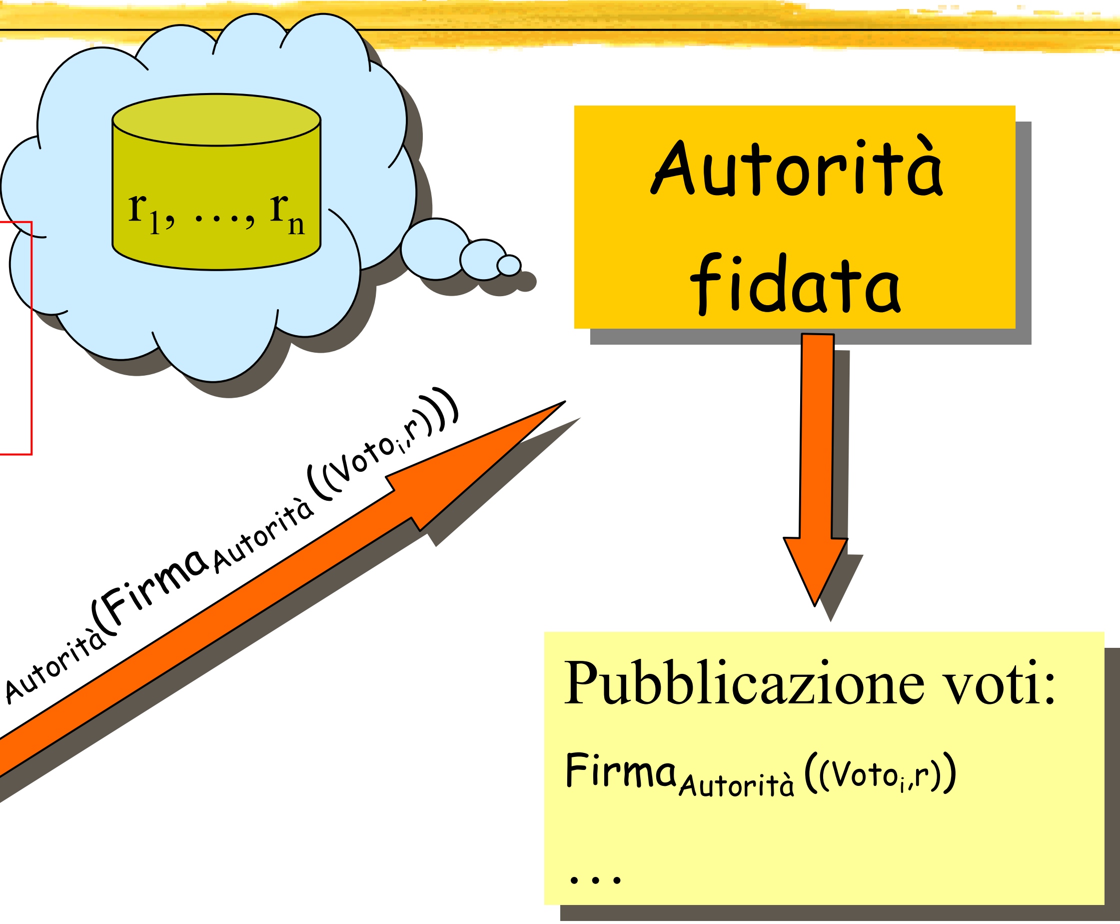
Elezioni III

Problemi?

Autorità (poco) "fidata"

-Aggiungere voti

-Modificare i voti



Posta elettronica

L' e-mail consente un rapido scambio di messaggi tra due utenti ma:

- L' integrità e l'autenticità del messaggio non sono garantite
- Non si può provare di aver spedito/ricevuto un messaggio
- Il canale di comunicazione è insicuro

Posta ordinaria

La raccomandata con ricevuta di ritorno garantisce che

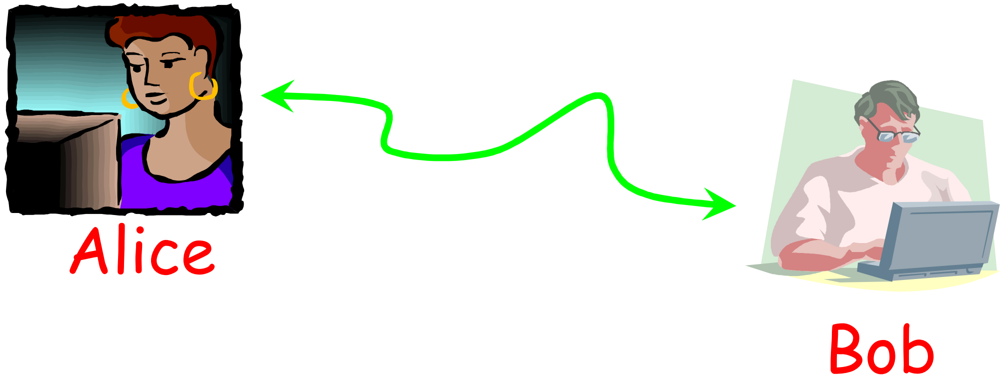
- Il mittente abbia una ricevuta di spedizione e una ricevuta di consegna
- Il ricevente ottenga il messaggio
- Le ricevute possano essere mostrate ad un giudice

La ricevuta indica che è stato spedito qualcosa, ma non dipende dal contenuto del messaggio!

Certified e-mail

Partecipanti:

- Alice (sender)
- Bob (receiver)



Inoltre:

- Terza parte fidata TTP
- Time Stamping Server TSS

Il ruolo del TTP

I protocolli di certified e-mail possono essere classificati in base al ruolo del TTP

- *Protocolli In-Line*
  - TTP on-line e totalmente fidato
- *Protocolli Ottimistici*
  - TTP interviene solo in caso di disputa tra le parti

TTP

Protocolli di fair-exchange

Ogni utente ha un segreto ed è interessato nel segreto dell'altro utente

Soluzione classica

- Scambio graduale di info tra le parti

Fair exchange

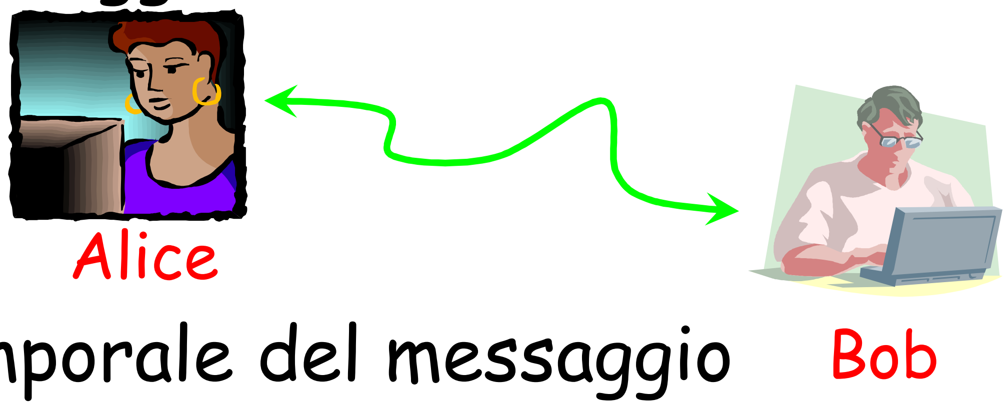
- *Entrambe le parti ottengono il segreto desiderato oppure*
- *Nessuna delle due ottiene alcuna informazione utile*

CEM basati su scambio graduale di info

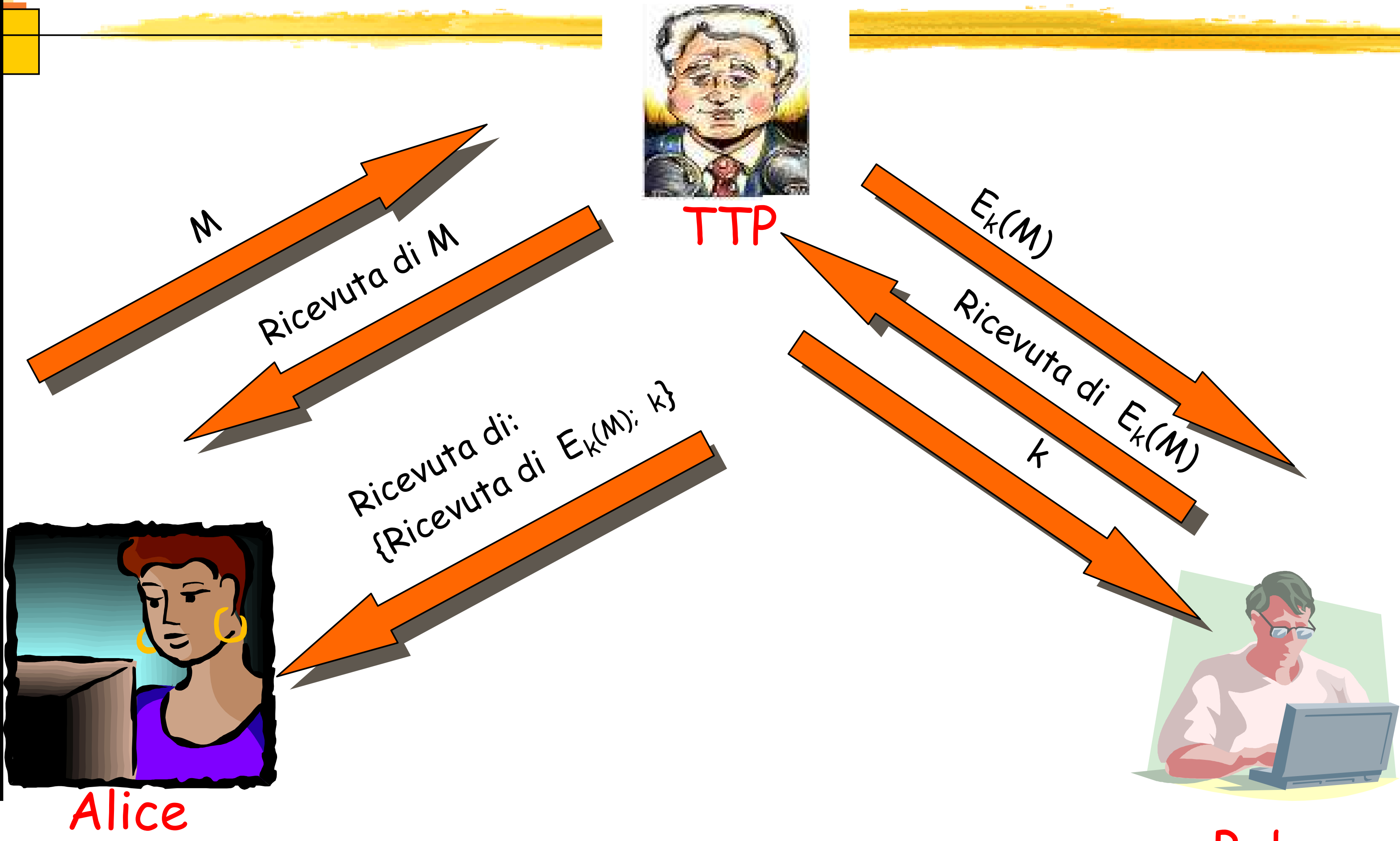
- Richedono un canale di comunicazione real-time e interattivo
- I sistemi di email sono asincroni e store-and-forward

Certified email: proprietà

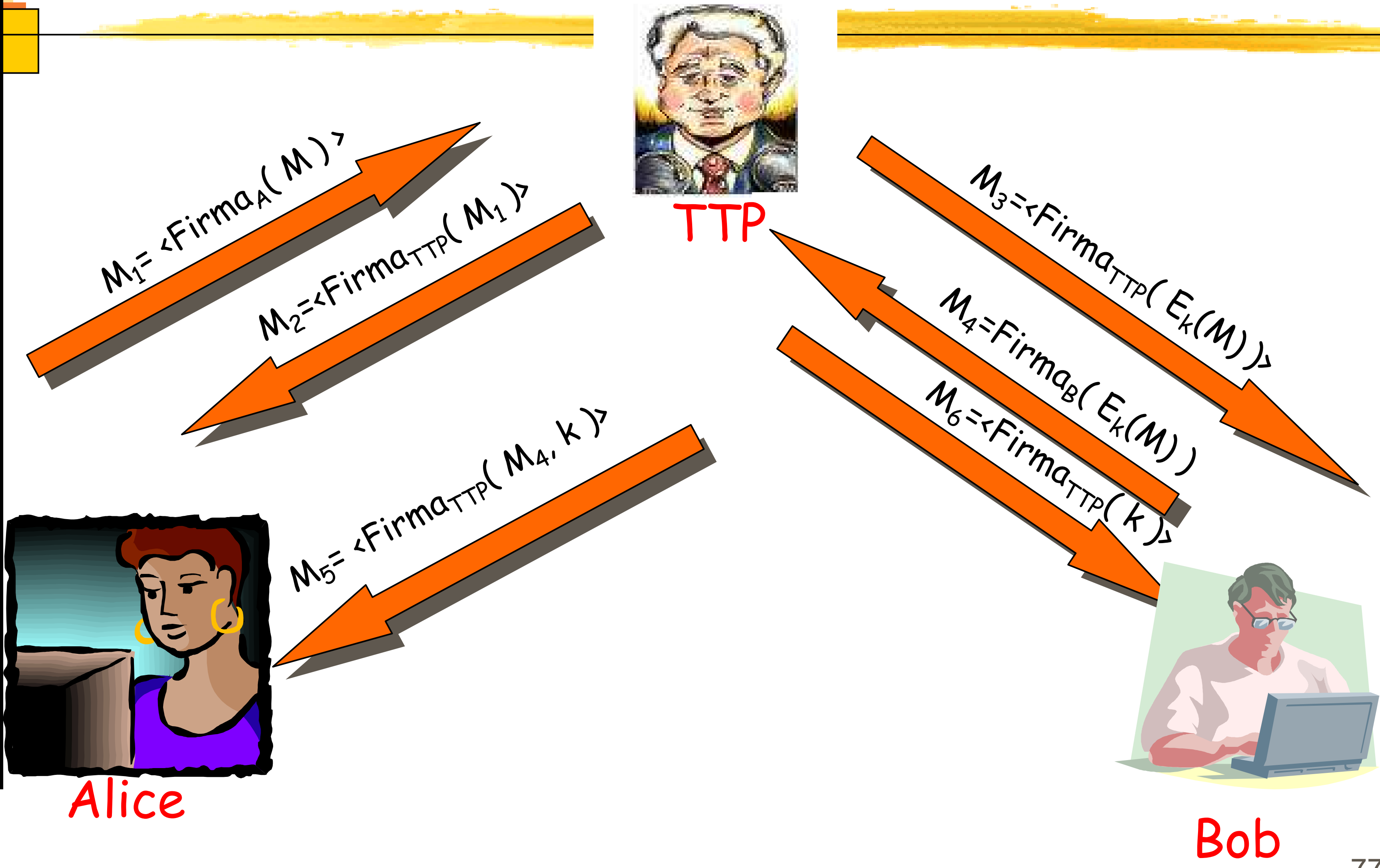
- Fairness
- Ricevuta di spedizione
- Non ripudio dell'origine
- Non ripudio della ricevuta
- Autenticità del messaggio
- Integrità
- Confidenzialità
- Timeliness
- Autenticazione temporale del messaggio



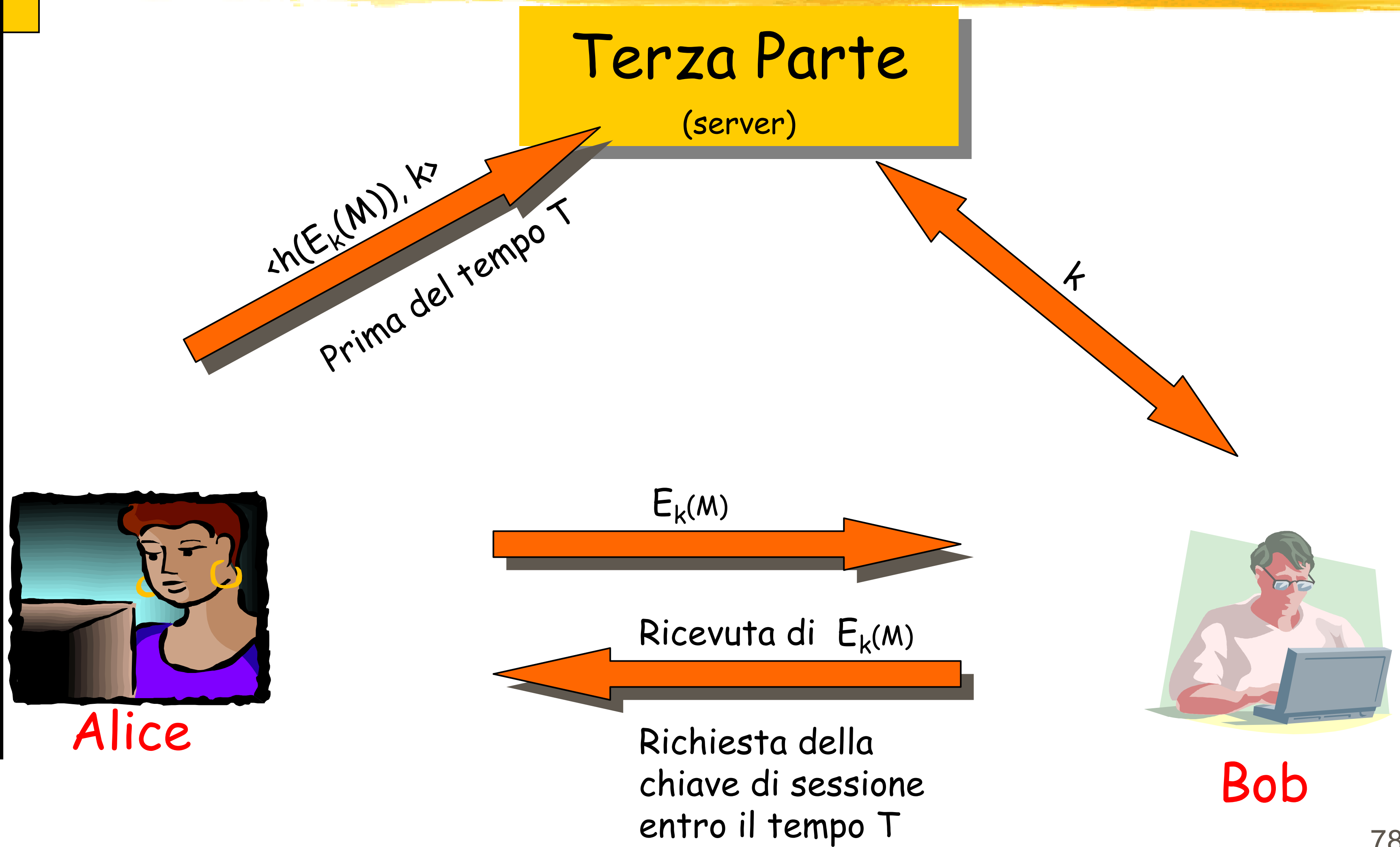
Protocollo inline Bahreman-Tygar



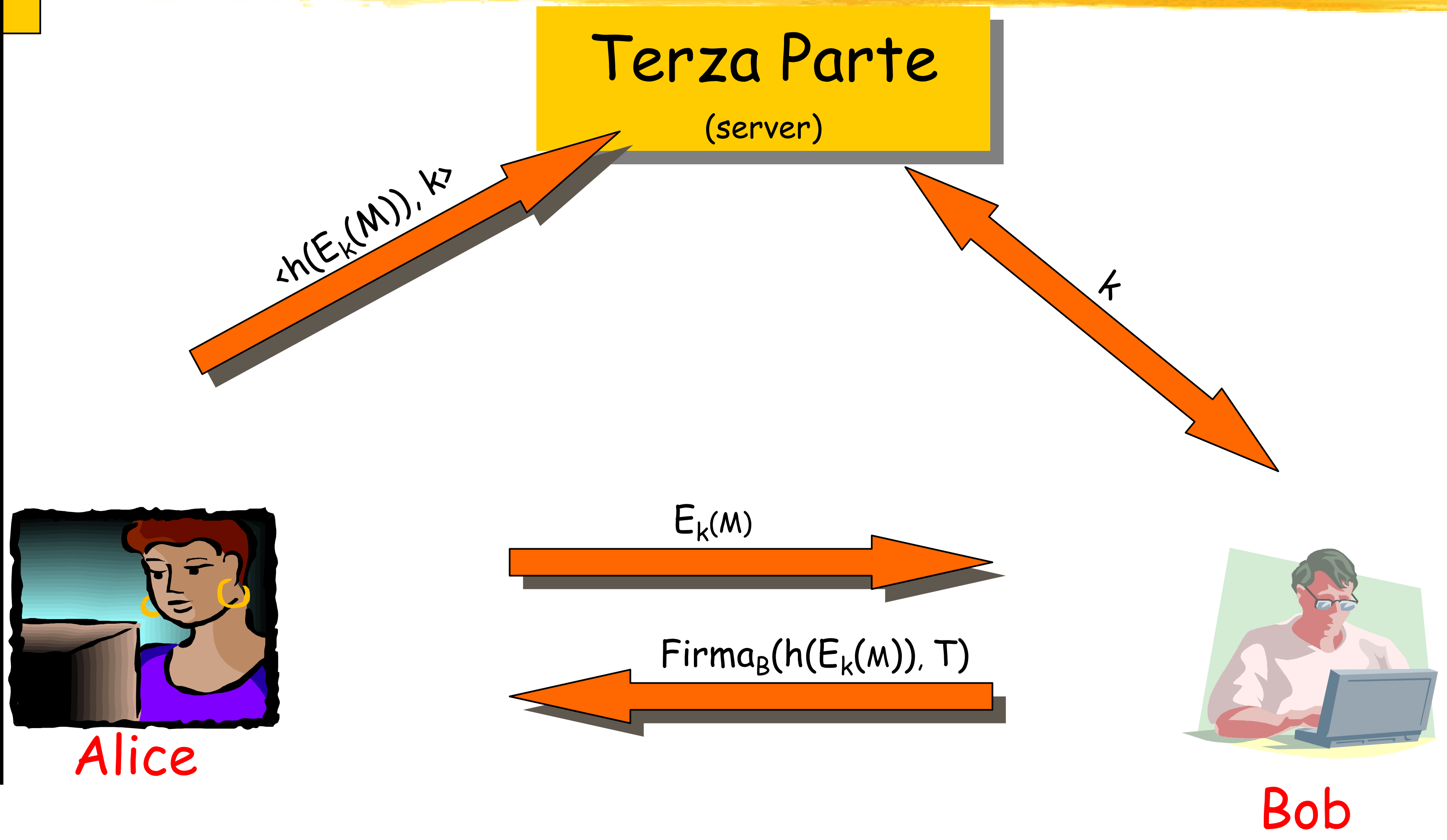
Protocollo inline Bahreman-Tygar



Protocollo in-line
Riordan - Schneier

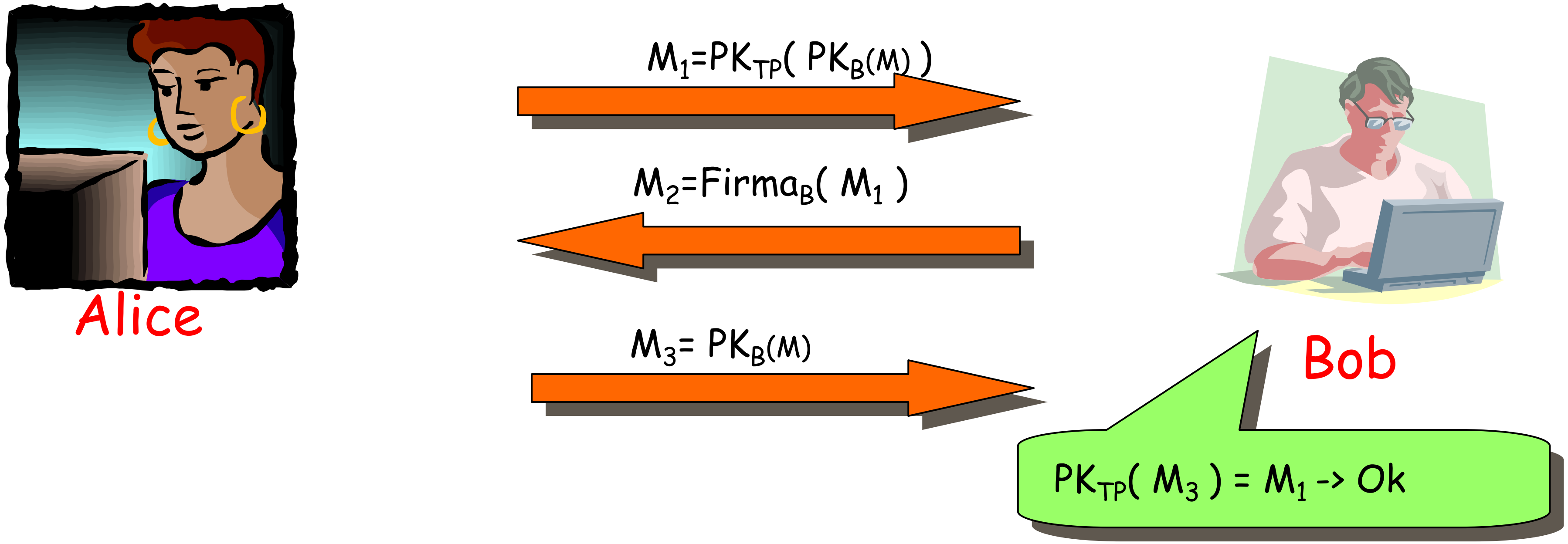


Protocollo in-line
Riordan - Schneier



Protocollo ottimistico

Micali



Protocollo ottimistico

Micali