Complementi di Sicurezza su Reti

Lezione tenuta dal
Prof. P. D'Arco

Presentazione di:

D'Alessio Fabio
Rocco Gaetano

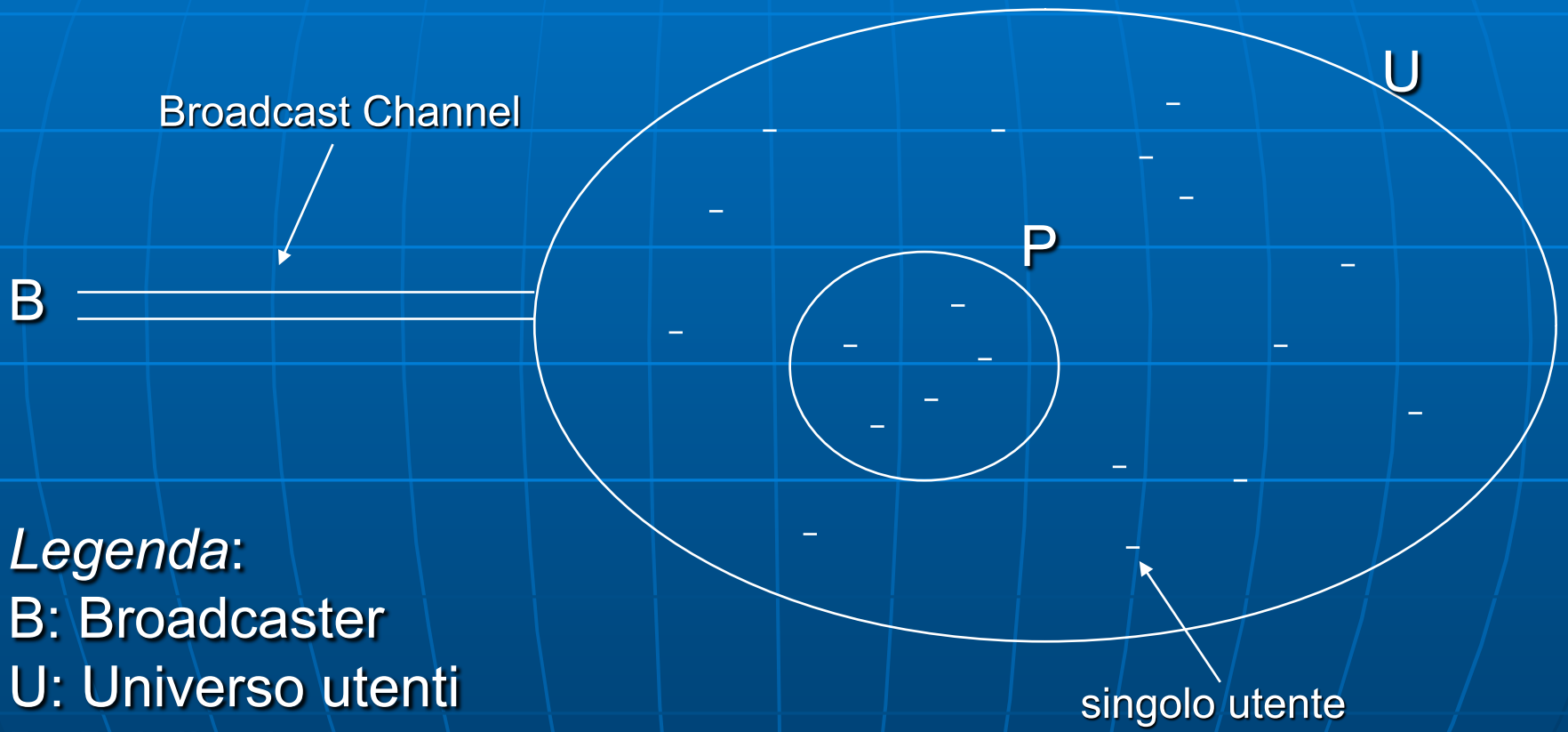
Obiettivi del corso:

- Studio di tecniche crittografiche per problemi di sicurezza e privatezza in alcuni domini applicativi
- Studio di strumenti matematici che rendono possibile un'implementazione efficiente di primitive crittografiche

Contenuti

- Schemi per trasmissioni broadcast sicure
- Primitive e Protocolli crittografici basati su curve ellittiche
- Tecnologia RFID: Autenticazione
- Secure two-party computation

Trasmissioni broadcast sicure



Legenda:
B: Broadcaster
U: Universo utenti
P: Privilegiati

Trasmissioni broadcast sicure

Tutti gli utenti u in U ricevono il messaggio inviato

Proprietà:

- Ogni utente u in P riesce a decifrare il messaggio di B
- Ogni coalizione di utenti R in U\P non riesce ad avere alcuna informazione sul messaggio

Applicazioni nel mondo reale:

- Pay per View
- CD, DVD, HD-DVD, Blu-Ray

Trasmissioni broadcast sicure

Prima soluzione

- B condivide con ogni utente u in U una chiave crittografica K_U
- All'inizio di ogni sessione, definito l'insieme dei privilegiati $P=\{u_1,u_2,\ldots,u_n\}$, B cifra il messaggio M una volta per ogni utente di P

$B \rightarrow P$ $\quad\quad C= E_{Ku_1}(M) \,||\, E_{Ku_2}(M) \,||\, \ldots || \, E_{Ku_n}(M)$

Problemi:

- B deve memorizzare n chiavi
- La taglia del messaggio è proporzionale al numero degli utenti
- Bisogna cifrare n volte il messaggio

Trasmissioni broadcast sicure

Seconda soluzione

- B genera per ogni $P \in 2^U \setminus \{0\}$ una chiave crittografica
- Assegna ad $u \in U$ l'insieme delle chiavi associate ai sottoinsiemi a cui appartiene, i.e., $\{K_s \mid S \subseteq U; u \in S\}$
- All'inizio di ogni sessione, fissato P, cifra ed invia:

$$C = E_{K_P}(M)$$

Problemi:

- B memorizza $\sum_{i=1}^{n} \binom{n}{i} = 2^n - 1$ con n=|U|

- Ogni $u \in U$ memorizza $1 + \sum_{i=1}^{n-1} \binom{n-1}{i} = 1 + 2^{n-1} - 1 = 2^{n-1}$

B.E.S.
(Broadcast Encryption Scheme)

Parametri per la valutazione delle prestazioni di uno schema crittografico

1. # chiavi memorizzate da ogni utente
2. # chiavi memorizzate dal broadcaster
3. lunghezza del testo cifrato C
4. # cifrature/decifrature effettuate da B e da $u \in P$

B.E.S.
(Broadcast Encryption System)

	Prima Soluzione	Seconda Soluzione
①	1	2^{n-1}
②	n	2^n-1
③	|P|	1
④	|P|	1

… cercheremo soluzioni intermedie rispetto a questi due estremi

Trasmissioni broadcast sicure

Problemi che affronteremo:

- Progettare schemi BES efficienti rispetto alle misure individuate

In particolare:

- Assumeremo che la maggior parte degli utenti $u \in U$ sia autorizzata alla ricezione e un insieme R debba essere efficientemente revocato
- Schemi statici (le chiavi che l'utente memorizza non cambiano nel tempo)

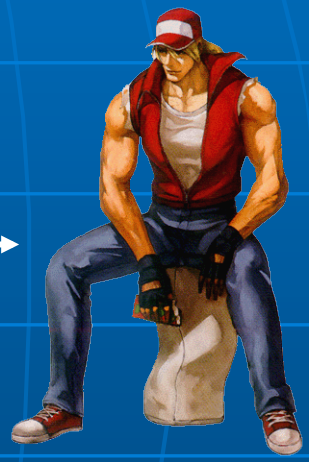
Argomenti trattati

- Schemi per trasmissioni broadcast sicuri
- Primitive e Protocolli crittografici basati su curve ellittiche
- Tecnologia RFID → Autenticazione

Protocolli crittografici basati su curve ellittiche



$C = E_{P_B}(M)$



Alice



Oscar

Bob

PB: chiave pubblica di BOB

Schemi di cifratura asimmetrica …

ElGamal	RSA
Primo p di 1024 bit	N = p · q di 1024 bit
Testo cifrato: 2048 bit	Testo cifrato: 1024 bit
Operazione principale: *esponenziazione modulare*	Operazione principale: *esponenziazione modulare*
Assunzione: *DLP*	Assunzione: *Fattorizzazione*

Assunzioni…

DLP

Z_p^*, con g generatore di Z_p^*

Dato y è computazionalmente difficile calcolare x tale che $g^x = y$

Fattorizzazione

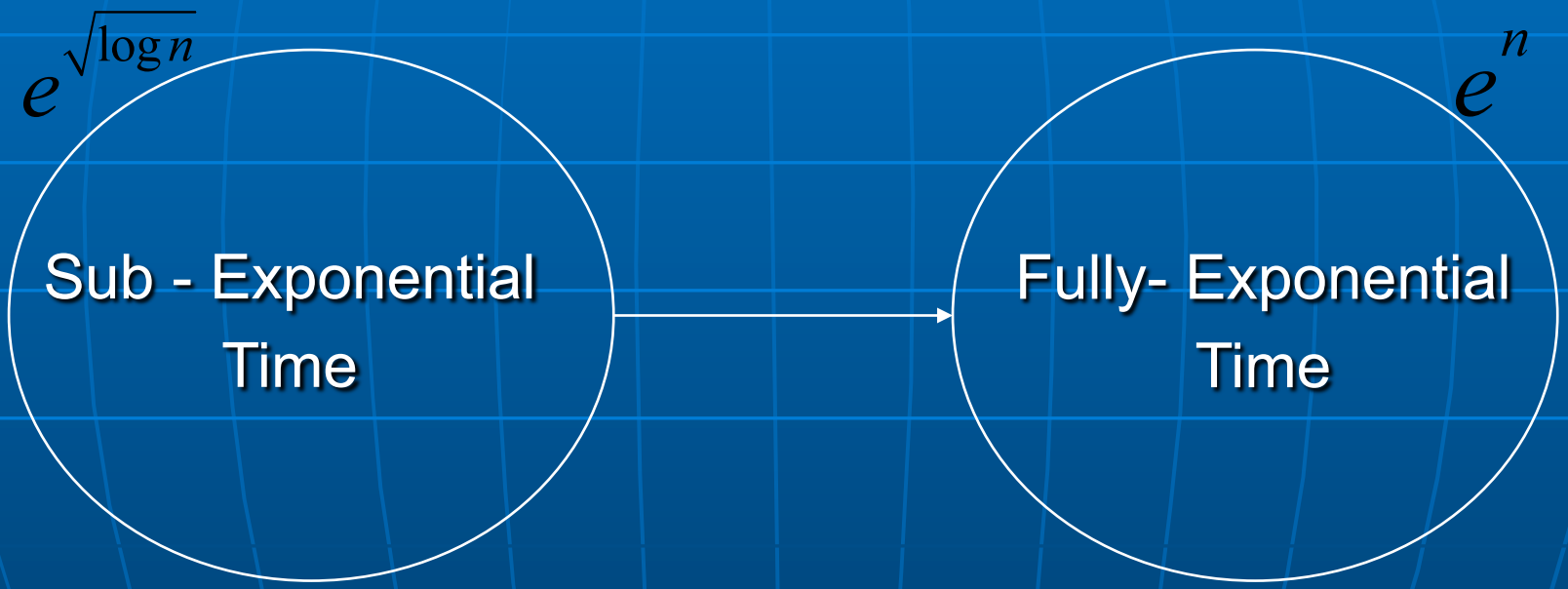
Dato N è computazionalmente difficile calcolare i fattori primi p e q

Possiamo fare meglio?

- Possiamo progettare uno schema in cui la cifratura/firma siano più piccole in termini di bit?
- Possiamo progettare uno schema computazionalmente più efficiente?
- Possiamo progettare uno schema con lo stesso grado di sicurezza?

Possiamo trovare “ambienti” in cui i migliori algoritmi “d’attacco” ai problemi difficili hanno performance peggiori di quelli per gli ambienti tradizionali

Complessità degli attacchi



Obiettivo

Invece di lavorare in Z_p^* vogliamo trovare un gruppo in cui DLP sia ancora più difficile da risolvere

L'insieme E(a,b) dei punti (x,y) appartenenti alla curva ellittica (in un campo finito)

$$y^2=x^3+ax+b$$

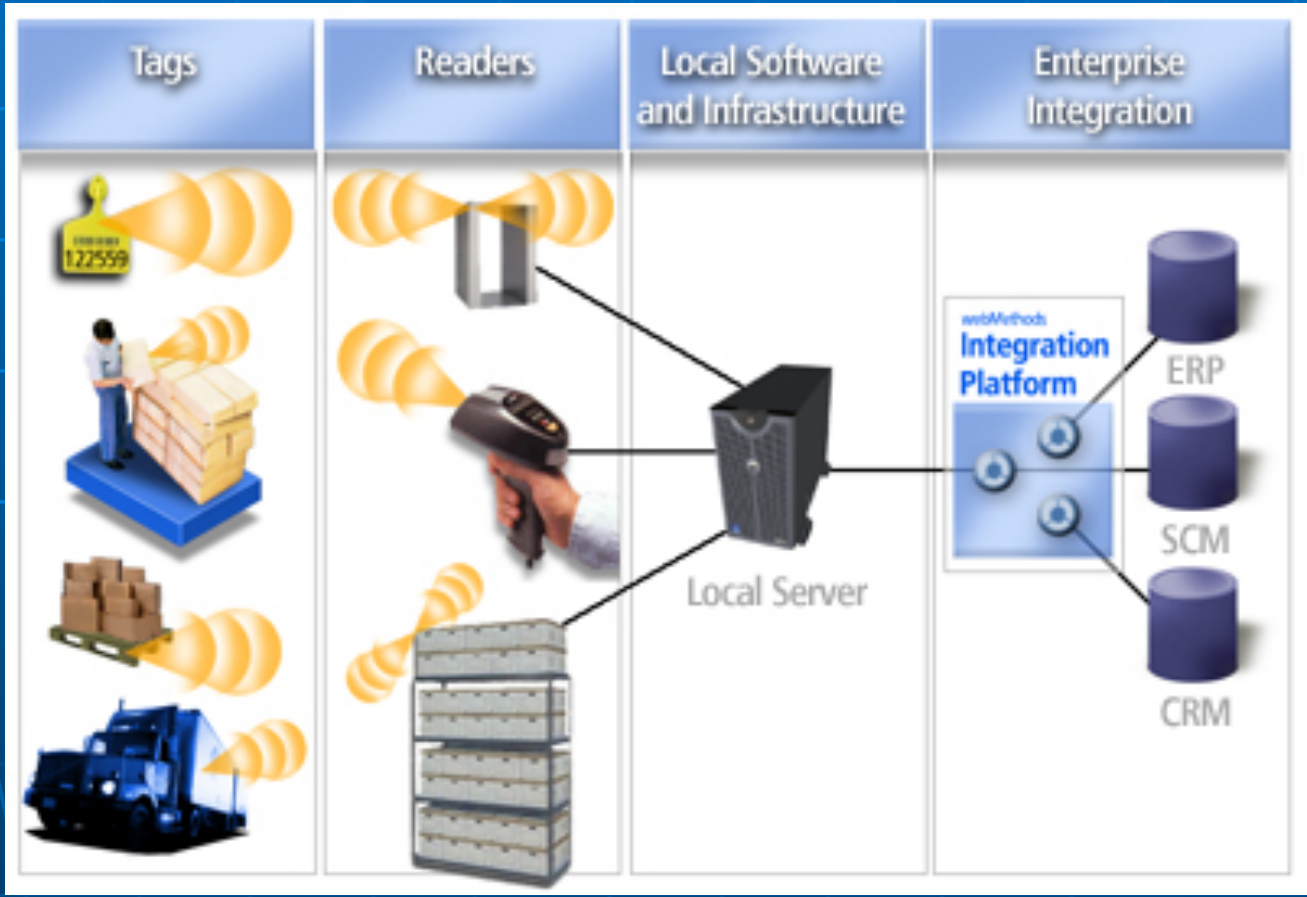
con operazioni opportunamente definite, fa al caso nostro

Argomenti trattati

- Schemi per trasmissioni broadcast sicuri
- Primitive e Protocolli crittografici basati su curve ellittiche
- Tecnologia RFID → Autenticazione

Tecnologia RFID

RFID è l'acronimo di Radio Frequency IDentification ed è una tecnologia usata per l'identificazione automatica degli oggetti



Tecnologia RFID

Il **TAG** è un'etichetta associata ad un oggetto recante informazioni per l'identificazione univoca
Dotato di circuiteria elementare e memoria

Esistono due tipi di TAG:

- *TAG passivo:* è sprovvisto di batteria e si ricarica quando è a una certa distanza dal reader
- *TAG attivo:* è provvisto di batteria per l'alimentazione

Il **Reader** ha la funzione di inviare query al TAG e quest'ultimo risponde inviando le informazioni che possiede in memoria

Tecnologia RFID

Applicazioni

- Identificazione automatica degli oggetti
- Inventario
- Tracciamento dei beni

Costruire un Reader illegale non è tecnicamente difficile.

Anche contraffare e produrre TAG clonati non è difficile

Tecnologia RFID

Applicazioni a rischio:

- Distribuzione dei farmaci

Problema:

- Occorre individuare protocolli Reader-Tag che assicurino l'autenticità della comunicazione

In particolare ci occuperemo di protocolli di autenticazione efficienti e sicuri per RFID

Argomenti trattati

- Schemi per trasmissioni broadcast sicuri
- Primitive e Protocolli crittografici basati su curve ellittiche
- Tecnologia RFID → Autenticazione
- Secure two-party computation

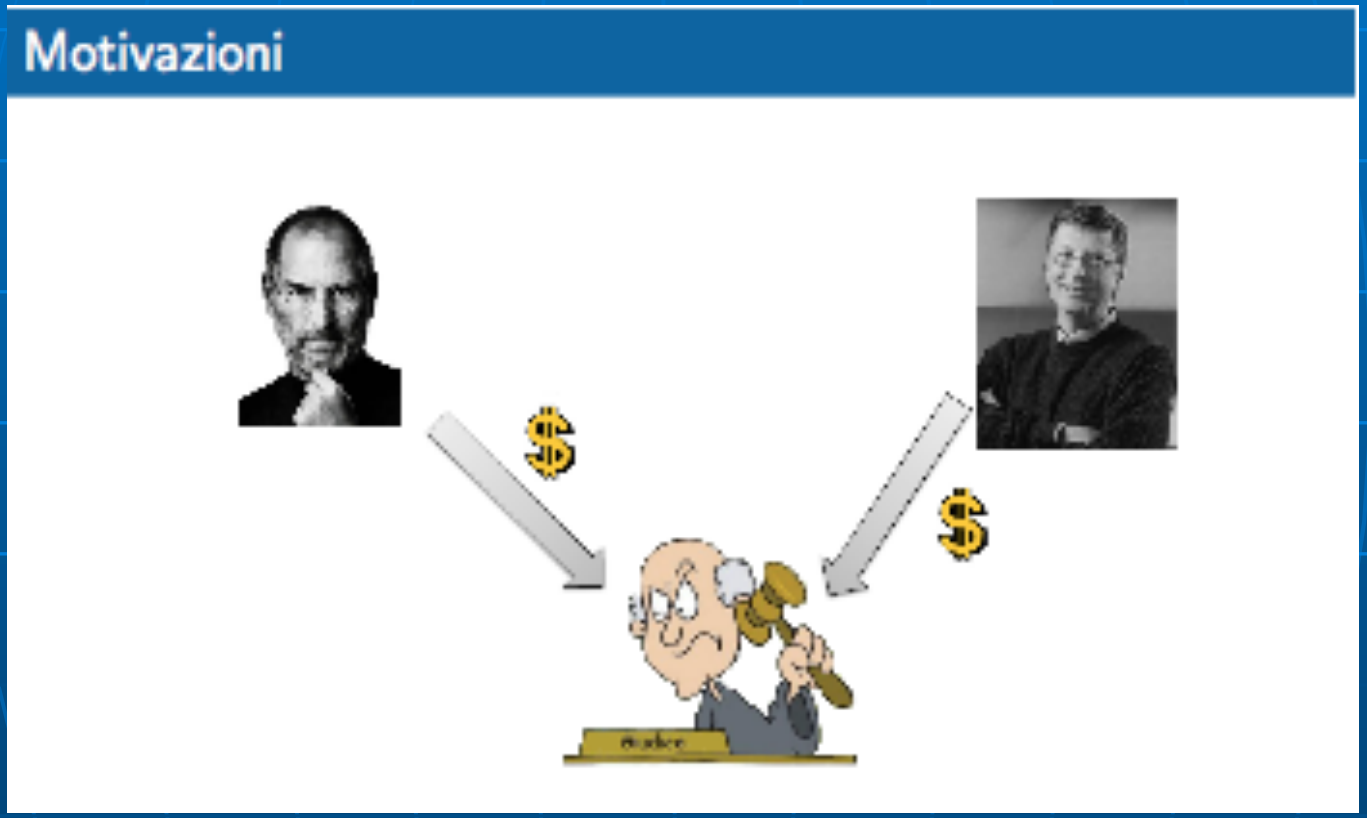
Problema dei milionari

Motivazioni



- Chi è più ricco?
- Nessuno dei due intende rivelare la propria ricchezza!

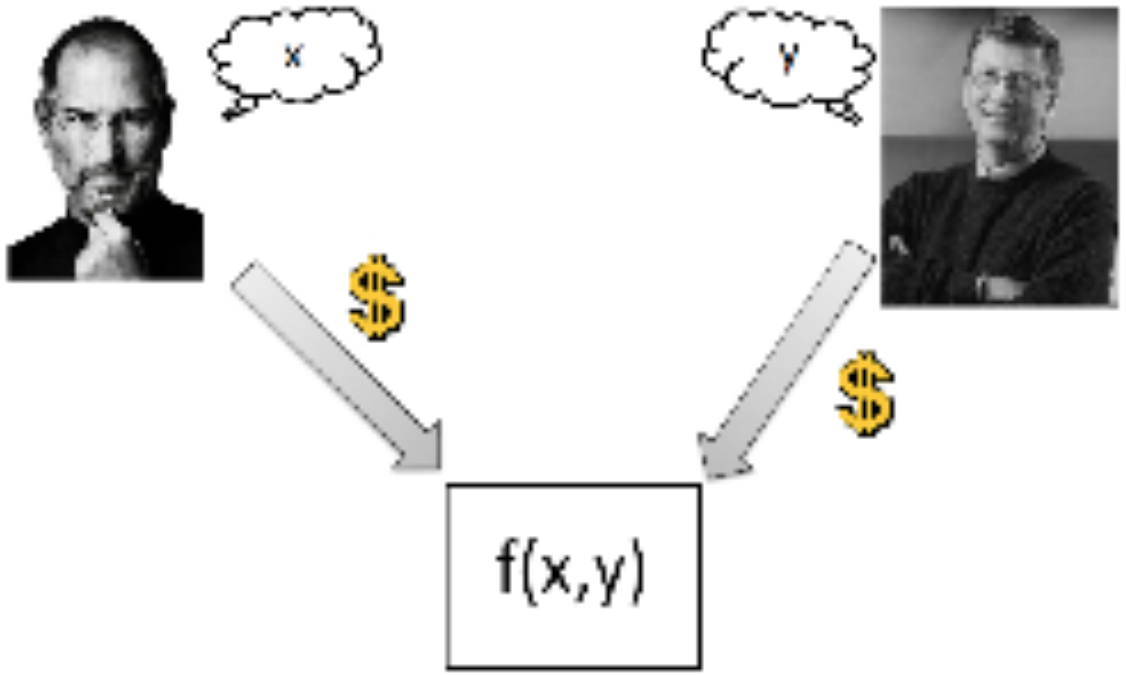
Soluzione: uso di una parte fidata



Obiettivo

- Vogliamo risolvere il problema **senza l'uso di una parte fidata**
- Serve un protocollo che le due parti possano eseguire che *emuli* la presenza di una terza parte fidata

Problema Generale



- Le due parti desiderano calcolare $f(x, y)$ mantenendo i propri input x e y privati

Setting

- P_1 ha input $x \in \{0,1\}^n$
- P_2 ha input $y \in \{0,1\}^n$
- $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$
- P_1 e P_2 vogliono calcolare congiuntamente $f(x,y)$, in modo tale che:
  - $\Rightarrow$ la computazione dia $f(x,y)$ e nessuna *informazione* sugli input x e y che non *possa* essere dedotta dalla conoscenza di $f(x,y)$