

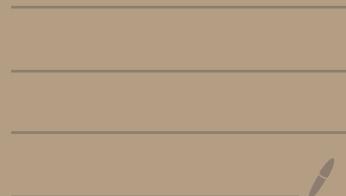
# CRITTOGRAFIA

---

lezione di lunedì 30/11

ore 11:15

- Protocolli a cono scena zero
- SSL



# Protocollo a Conoscenza Zero (Zero-Knowledge)

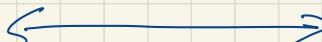
Silvio Micali, Shafi Goldwasser

MIT

1989

PROVER

Peggy



VERIFIER

Victor

ESEMPIO

Ronito  
Graenelli' di Sibiu

PREPARAZIONE



PF

b0 = Ronito dei  
Graenelli' di Sibiu

## Protocollo

for  $i = 1$  to  $k$  } //  $k$  scelto da  $V$

P si volte

$V$  sceglie  $e \in \{0, 1\}$  a caso

if ( $e == 0$ )  $V$  toglie un granello di sabbia

$V$  chiede a  $P$  il nuovo valore  $b_i$

if (( $e == 0$  &  $b_i \neq b_{i-1}$ ) ||  
 $(e == 1$  &  $b_i == b_{i-1})$ )

CONTINUA ALLA PROSSIMA ITERAZIONE

else

"P è un impostore"

STOP

}

"P dice J vero con probabilità  $1 - \left(\frac{1}{2}\right)^k$ ".

Probabilità di ingannare  $V$ : = probabilità di procedere

Concretamente il bit generato, per  $k$  volte



$$\left(\frac{1}{2}\right)^k$$

Probabilità ~~di~~ che P obbia la capsule assente

$$\text{è almeno } 1 - \left(\frac{1}{2}\right)^k$$

## PRINCIPI GENERALI DEI PROTOCOLLI ZERO-K

### • CORRETTEZZA

Se  $P$  è onesto e la sua scommessa è vero,  $V$  ne accetta sempre la dimostrazione.

### • CORRETTEZZA



## CORRETEZZA

Se l'affermazione di  $P$  è falsa ( $P$  è dishonesto),  $V$  può essere ~~costretto~~ ingannato con probabilità  $\leq \left(\frac{1}{2}\right)^k$ , dove  $k$  è scelto da  $V$ .

## CONOSCENZA - ZERO

Se l'affermazione di  $P$  è vera, il verificatore  $V$  (anche se dishonesto) non può ~~scegliere~~ acquisire alcuna informazione se non la veridicità di questo fatto.

## Protocollo di identificazione zero-k.

### PROTOCOLLO DI PLAT-SHAMIR

- P dimostra a V la sua identità senza rivelare alcun'altra informazione.
  - basato sulla difficoltà di calcolo delle  $\sqrt{}$  in moduli  $n$ ,  
 $n$  composto
- $$t = s^2 \bmod n$$
- $n$  composto.

V: conosce  $t, n$

P: convince V di conoscere le  $\sqrt{}$  di t

### PREPARAZIONE

P sceglie p e q primi

calcola  $n = p \cdot q$ , e sceglie  $s < n$

$$t = s^2 \bmod n$$

P rende nōs la copia  $\langle t, n \rangle$  (chiave pubblica)

mentiene segreta  $\langle p, q, s \rangle$  (chiave privata)

### Protocollo

Ripeti k volte:

1) V chiede a P di iniziare una iterazione

2) P genera un intero  $r < n$  casuale

$$\text{calcola } u = r^2 \bmod n$$

comunica  $u$  a V

3) V genera  $e \in \{0, 1\}$  casuale  
comunica  $e$  a P

4) P calcola  $z = r \cdot s^e \bmod n$   
e comunica  $z$  a V

5) V calcola  $x = z^2 \bmod n$

if ( $x == ut^e \bmod n$ ) ripete da 1)

else STOP // P non è identificato

$$\// e=0$$

$$z=r$$

$$\// e=1 \quad z = r \cdot s \bmod n$$

$$\// (r \cdot s^e)^2 = r^2 (s^e)^2 = \\ = u \cdot (s^2)^e = u t^e$$

## Complezione

$$\text{Ora: } e=0 \Rightarrow x = ut^e \bmod n = u \bmod n$$

$$e=1 \Rightarrow x = z^2 \bmod n = (rs^e)^2 \bmod n = ut \bmod n$$

P supera tutte le sfide, V aspetta la dimostrazione

## Corretto

ESEMPIO

V manda sempre  $e=1$

P si aspetta di ricevere  $e=1$

al punto 2 sceglie  $r$ , a caso

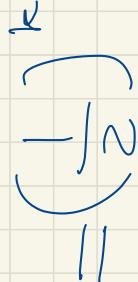
$$\text{e invia a V} \quad u = \frac{r^2}{t} \bmod n = r^2 t^{-1} \bmod n$$

al punto 4 invia  $z = r \bmod n$

Venice di V:

$$x = z^2 \bmod n$$

$$x = ? \quad ut^e = ut \\ e=1$$



$$x = z^2 \bmod n = r^2 \bmod n$$

$$ut = \left( \frac{r^2}{t} \right) \cdot t \bmod n = r^2 \bmod n$$

$$x = ut \quad \checkmark$$

Protocollo  
comunicazione

### CORRETTEZZA

- Per discorrere necessita di ingannare V se prende correttamente il bit e inviato da V ad ogni iterazione
- Poiché' è generato casualmente, le previsioni di P sono corrette con probabilità 1/2 ad ogni iterazione