

---

---

---

---

---



## Protocollo zero-knowledge

Peggy P

prover

CORRETTEZZA

Se  $P$  è onesto, e la sua affermazione è vero,  $V$  accetta sempre la dimostrazione

Victor V

verif

CORRETTEZZA

Se  $P$  è disonesto (la sua affermazione è falso),  $V$  può essere ingannato con probabilità  $\leq (\frac{1}{2})^k$ ,  $k$  scelto da  $V$

CONOSCENZA ZERO

Se l'affermazione di  $P$  è vera, un verificatore onesto disonesto non può acquisire alcuna informazione se non la verifica dell'affermazione

# PROTOCOLLO DI PLAT-SHAMIR (Identificazione)

basato sulla difficoltà del calcolo delle radici quadrate verificate senza compito.

## PREPARAZIONE

P sceglie  $p \neq q$  primi molto grandi

calcola  $n = p \times q$

sceglie  $s < n$

calcola  $t = s^2 \bmod n$

$s$  = segreto (chiave privata)  
di P

rende nota  $\langle t, n \rangle$   $\rightsquigarrow$  chiave pubblica

man tiene privata  $\langle p, q, s \rangle$   $\rightsquigarrow$  chiave privata

## PROTOCOLLO

ripeti  $k$  volte //  $k$  scelto da  $V$

1)  $V$  chiede a  $P$  di iniziare una iterazione (stato)

2)  $P$  sceglie  $r < n$  random

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

comunica  $u \in V$

3)  $V$  genera un bit  $e \in \{0, 1\}$  random  
e lo comunica a  $P$

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

$$e=0 \Rightarrow z = r \bmod n$$

$$e=1 \Rightarrow z = r \cdot s \bmod n$$

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

if ( $x = u \cdot t^e \bmod n$ ) fine al passo 1)

else \*STOP\* //  $P$  non è identificato

## CORRETTEZZA

$$e = 0$$

$$\underline{x = ut^e \bmod n = u \bmod n}$$

$$e = 1$$

$$x = (2^r) \bmod n = (rs^e)^2 \bmod n = ut \bmod n$$

P suppone retta le sfide se conosce s

## CORRETTEZZA

P disonesto (non conosce s)

1° caso

P prende di nascosto e = 0

esegue il protocollo senza modificarlo

se la precisione è corretta, P suppone le sfide

2° caso

P prende di ricovero  $\neq e=1$

P cambia il passo 2 del protocollo:

2') P inizia  $u = r^2 \times t^{-1} \bmod n$

e al passo 4 invia  $z = r \bmod n$

al passo 5, se la precisione di Pe'

Corretta, P ripete lo stesso:

infatti

$$V \text{ controlla } x = z^2 = u \cdot t^e \stackrel{e=1}{=} ut$$

$$z^2 = (r)^2 = r^2$$

$$(r^2 \times t^{-1}) \times t = r^2$$

$\Rightarrow$  P dishonesto riesce a ingannare V se è in grado di predire i bit e

se i bit e sono generati correntemente,

P inganna V con probabilità  $(\frac{1}{2})^k$

Al punto 2) mondo  $u = \frac{r^2}{t} \bmod n$

Al punto 4) mondo r

Al punto 5: V controlla se

$$\cancel{x = z^2 = r^2} \quad ? \quad \cancel{u t^e = \left(\frac{r}{t}\right)^2}$$