Protocollo Fiat-Shamir

Protocollo di identificazione a conoscenza zero basato sulla difficoltà dell'estrazione di radice modulo un numero composto.

Preparazione

P:

- sceglie p e q primi molto grandi;
- calcola $n = pq$;
- sceglie $s < n$ segreto (chiave privata);
- calcola $t = s^2 \bmod n$;
- rende nota la coppia (t, n).

Protocollo

Ripetuto k volte, con k scelto da V:

1. V chiede a P di iniziare una iterazione;
2. P sceglie $r < n$ casuale, calcola $u = r^2 \bmod n$ e lo comunica a V;
3. V genera un bit e *casuale* e lo comunica a P;
4. P calcola $z = rs^e \bmod n$ e invia z a V (se $e = 0$ allora $z = r$, altrimenti $z = rs$);
5. V calcola $x = z^2 \bmod n$; se $x = ut^e \bmod n$ va alla prossima iterazione, altrimenti stop (P non identificato).

Dimostrazione

completezza P supera tutte le sfide se conosce s:

$e = 0$ $x = ut^e \bmod n = u \bmod n$;
$e = 1$ $x = z^2 \bmod n = (rs^e)^2 \bmod n = ut \bmod n$;

correttezza supponendo che P sia disonensto:

- se $e = 0$, esegue il protocollo comunicando r;
- altrimenti cambia il passo 2 del protocollo, inviando

$$u = r^2 t^{-1} \bmod n,$$

e al passo 4 invia $z = r \bmod n$. P supera la prova: $x = r^2$ e

$$(r^2 t^{-1})t = r^2 = x.$$

P riesce a ingannare V a condizione di prevedere e: non può aspettare di riceverlo, visto che nel caso in cui $e = 1$ dovrebbe modificare retroattivamente il valore r che ha comunicato. Di conseguenza supera tutte le sfide con probabilità $\frac{1}{2^k}$;

conoscenza zero r è scelto da P. Se $e = 1$ non viene inviato a V, altrimenti questo potrebbe ricavare s calcolando $r^{-1}z \bmod n$.

t molto probabilmente è invertibile modulo n, visto che è un semiprimo e i valori usati sono grandi.