Protocolli zero-knowledge

Permettono ad un *prover* P di dimostrare a un *verifier* V di essere in possesso di una determinata capacità, senza rivelare dettagli sulla stessa. Questo avviene attraverso una serie di sfide proposte da V a P e con una componente casuale: se P fallisce una prova allora sicuramente non possiede la capacità, se le supera tutte probabilmente sì.

Caratteristiche:

completezza se P è onesto, V accetta sempre la dimostrazione;

correttezza se P è disonesto, la probabilità che riesca a ingannare V è al più $\frac{1}{2^k}$ con k scelto da V, quindi P non deve poter prevedere le sfide di V (casualità);

conoscenza zero se l'affermazione di P è vera, un verificatore anche disonesto non può acquisire alcuna informazione se non la veridicità dell'affermazione.