Identificazione su canale insicuro

Basata su cifrari asimmetrici. Supponendo di usare RSA, quando l'utente U con chiavi $k_{\text{pub}} = (e, n)$ e $k_{\text{priv}} = d$ richiede l'accesso al sistema S,

- S genera un numero casuale $r < n$ e lo invia in chiaro a U;
- U risponde con $f = r^d \bmod n$ (firma di U su r);
- S verifica la firma controllando che $f^e \bmod n = r$.

Stiamo cifrando con la chiave privata e decifrando con la chiave pubblica. Funziona perché le due operazioni sono commutative ($(x^e)^d \equiv (x^d)^e \equiv x \mod n$), e solo U può produrre un f adatto essendo l'unico a conoscenza di d.

Problema: se S è disonesto, r può essere scelto in modo da ricavare qualche informazione sulla chiave privata. Risolto con protocolli a conoscenza zero.