Chaum’s Blind Signature & Untraceable e-Cash

Pre-requisites: notes for RSA algorithm.



Blind Signing:

Scenario: Alice wants to have Bob’s signature on M.



Correctness:



Double-spending detection in e-Cash:

Each e-Cash coin contains two shares – S0 and S1.

S0 or S1 solely will not reveal payer’s identity, but the combination of two shares will.

Suppose S0 is a sequence of random bits, u is the bit string of payer’s real identity, then .

Due to the reversibility of XOR, .