Lecture 11

dinsdag 20 december 2022 10:36

payer pays to payee, who receives money

- different values
- transferable
- anonymous — not linked to owner
- Untraceable — serial number
- Unforgeable
- hard to duplicate

for an ecash scheme, we need

- withdrawal
- payment
- deposit

first attempt: signed (serial number, value)

second attempt: immediate deposit, payment succeeds if serial number not claimed before

- blinding — R prepares blinded message $M' = f(M)$
- signing — R sends M' to S; S replies with signature σ' on M'
- unblinding — R extracts signature σ for M from M'

one-more unforgability — l oracle calls does not imply l signatures

Unlinkability — signature cannot be connected to specific blinded message

RSA signatures require redundancy (e.g. from of hash)

↓

blind signature: but can still blind message by multiplying hash by invertible random constant

- multiply by r^e
- divide by r / multiply by r^{-1}

information-theoretically unlinkable

Unforgeability: random oracle issues due to blinding

denominations with relatively prime exponents

7^{th} root cannot be obtained from 3^{th} root and 5^{th} root

offline version: embed identity in each coin

challenge-response:

- Single run leaks no user information
- two runs leaks user identity