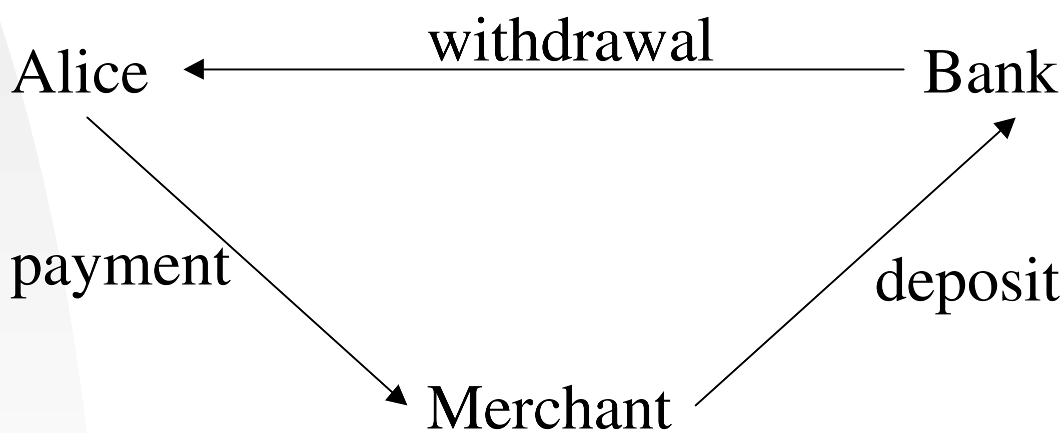
Digital Cash

Hua and Zhongtao

- Outline
  - What’s digital cash?
  - A simple E-cash system step-by-step
  - Desirable properties
  - Wallet with observer
  - Trustee-based Tracing
- Stop me whenever you feel unclear!

What's Digital Cash?

- Numbers that are money
- double spending / anonymity / offline



Ideal E-cash System

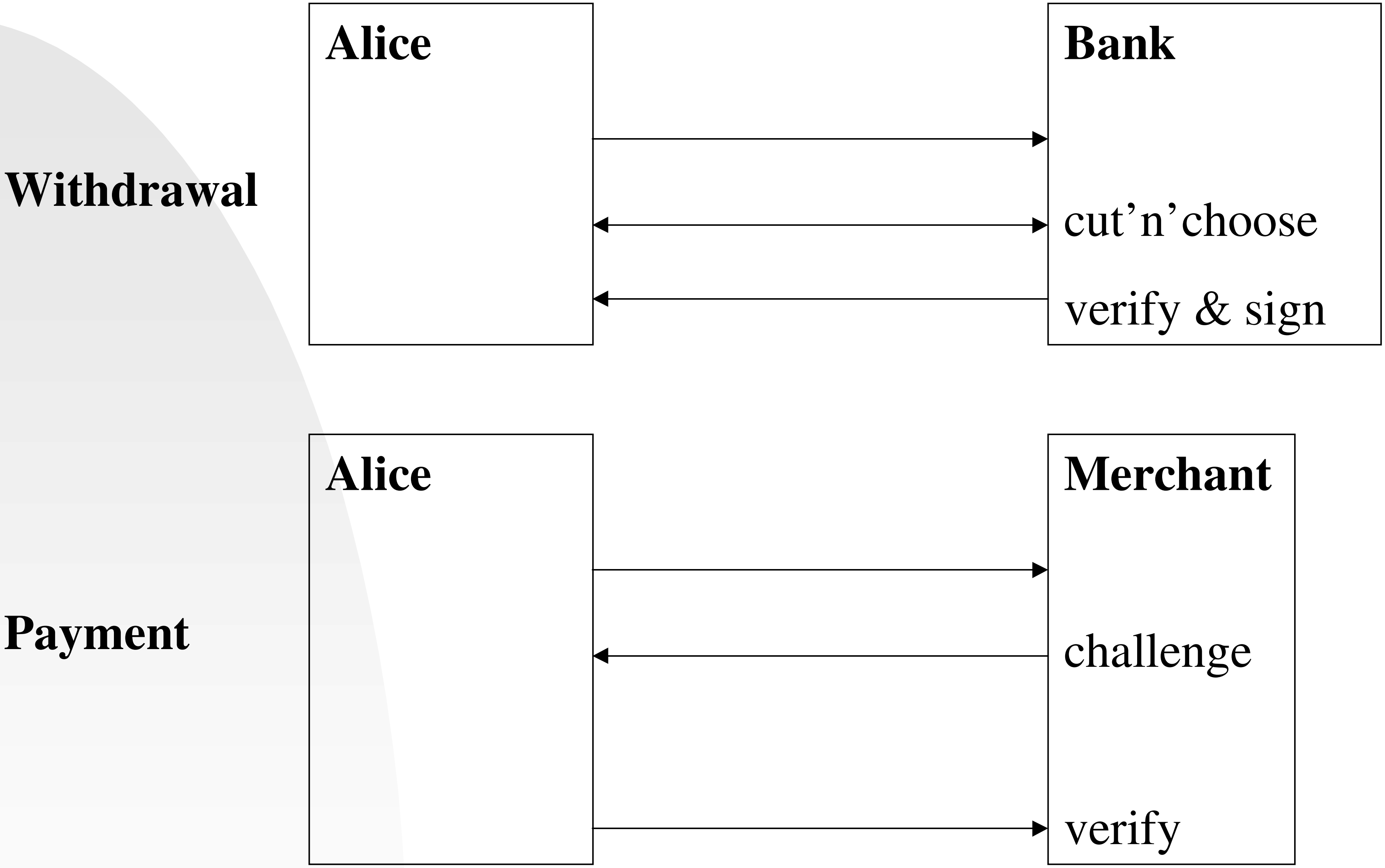
- Security: non-reusable, non-forgeable
- Privacy: non-traceable
- Off-line Payment
- Transferability
- Divisibility

Blind Signature

Have the bank sign the cash but remain anonymous

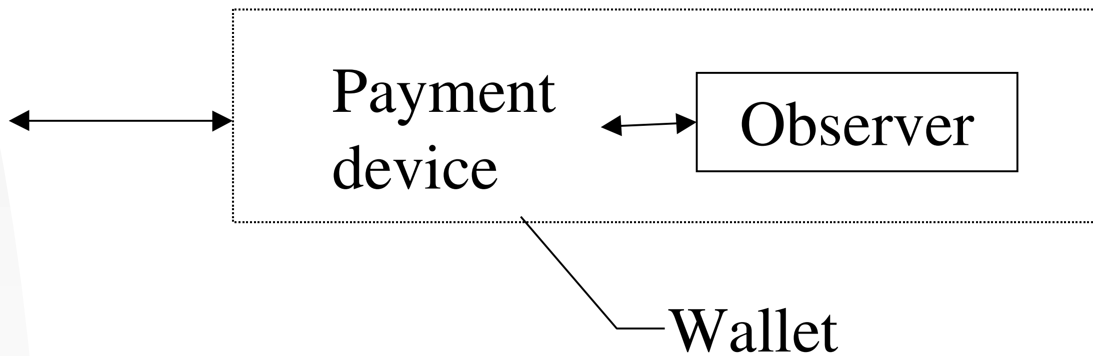
Wanna get: x,f(x) (mod n)

A really simple E-cash system [CFN90]



Wallet with Observers

- Prior detection of double spending
- Wallet = Payment device + Observer
- Anonymity concerns



Perfect Crime

- Alice kidnaps a baby
- Alice blinds the money and sends to authorities demanding:
  - Have a bank sign the money
  - Publish results in newspaper
- The authorities comply
- Alice buys a newspaper, unblinds the money, and starts spending them

Trustee-based Tracing

- Compromise between privacy and crime containment
- Traceable with the cooperation of Trustees (key-escrow agents)
- Incorporated into Brands' system ([BGK95])

Real Life

- Cybercash (http://www.cybercash.com)
- Digicash (http://www.digicash.com)
- NetBill

  (ask Doug)