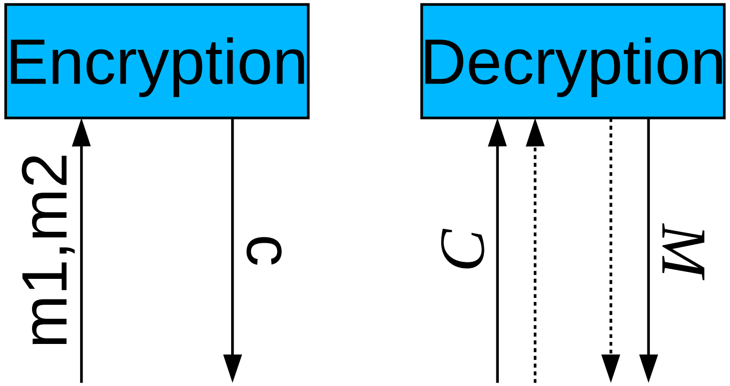
Provable Anonymous Networks

Evolution of Cryptography

- Classical Security
  - Try to find attacks
    - Found: System insecure
    - Not Found: Security unknown
- Provable Security
  - Define assumptions
  - Prove the absence of attacks
    - Not provable: Assumptions false
    - Provable: Secure under the assumptions
  - Reductions to prove security
    - Assume attacker can break the system
    - Construct an attacker breaking an assumption

Attacks on Cryptography

- Cryptographic security
  - Strongest attacker
  - Weakest goal
  - Negligible advantage
- Example: IND-CCA2
  - Chose two plaintexts
  - Distinguish ciphertexts
  - Use decryption oracle



c=m1 or m2?

Attacks on Anonymity

- Current anonymous networks
  - Reasonable attacker
  - Strong goals
    - Look at attacks individually
    - Provide countermeasures
  - Attacker can only learn little
    - But the whole is more than the sum of its parts...
- Provable anonymity
  - First approaches
  - Some proves on MIXes

What is a Strong Attacker?

- Derive any information
  - Timing
  - Distance
  - Location
  - ...
- Reduction to information/probability theory
  - Formal models are required
  - Verification, Model Checking

What are Reasonable Assumptions?

- Secure cryptography
  - Requires PKI
- Unobservability
  - Requires trust?
- Unlinkability
  - Prevent statistical evaluation

Back to GNUnet

- Very complex system
  - No formal model
  - No proves
- Broken by design
  - Unlinkability
  - Unobservability
- Leaks information
  - Even without attacks
  - Exploitable feature: Shortcuts

Comments, Questions?