Anonymity Networks

Vitaly Shmatikov

Privacy on Public Networks

- Internet is designed as a public network
  - Machines on your LAN may see your traffic, network routers see all traffic that passes through them
- Routing information is public
  - IP packet headers identify source and destination
  - Even a passive observer can easily figure out who is talking to whom
- Encryption does not hide identities
  - Encryption hides payload, but not routing information
  - Even IP-level encryption (tunnel-mode IPsec/ESP) reveals IP addresses of IPsec gateways

Applications of Anonymity (1)

- Privacy
  - Hide Web browsing and other online behavior from intrusive governments, advertisers, archivists
- Untraceable electronic mail
  - Political dissidents
  - Corporate whistle-blowers
  - Socially sensitive communications (online AA meeting)
  - Confidential business negotiations
- Law enforcement and intelligence
  - Sting operations and honeypots
  - Secret communications on a public network

Applications of Anonymity (2)

- Digital cash
  - Electronic currency with properties of paper money (online purchases unlinkable to buyer's identity)
- Anonymous electronic voting
- Censorship-resistant publishing
- Crypto-anarchy
  - "Some people say `anarchy won't work'. That's not an argument against anarchy; that's an argument against work." – Bob Black

What is Anonymity?

- Anonymity
  - Observer can see who is using the system and which actions take place (email sent, website visited, etc.), but cannot link any specific action to a participant
  - Hide your activities among others' similar activities
    - Anonymity is the state of being not identifiable within a set of subjects
  - You cannot be anonymous by yourself!
    - Big difference between anonymity and confidentiality
- Unobservability
  - Observer cannot even tell whether a certain action took place or not

Attacks on Anonymity

- Passive traffic analysis
  - Infer from network traffic who is talking to whom
  - Consequence: to hide your traffic, must mix it with other people's traffic
- Active traffic analysis
  - Inject packets or put a timing signature on packet flow
- Compromise of network nodes (routers)
  - It may not be obvious to a user which nodes have been compromised $\Rightarrow$ better not to trust any individual node
    - Assume that some fraction of nodes is good, don't know which

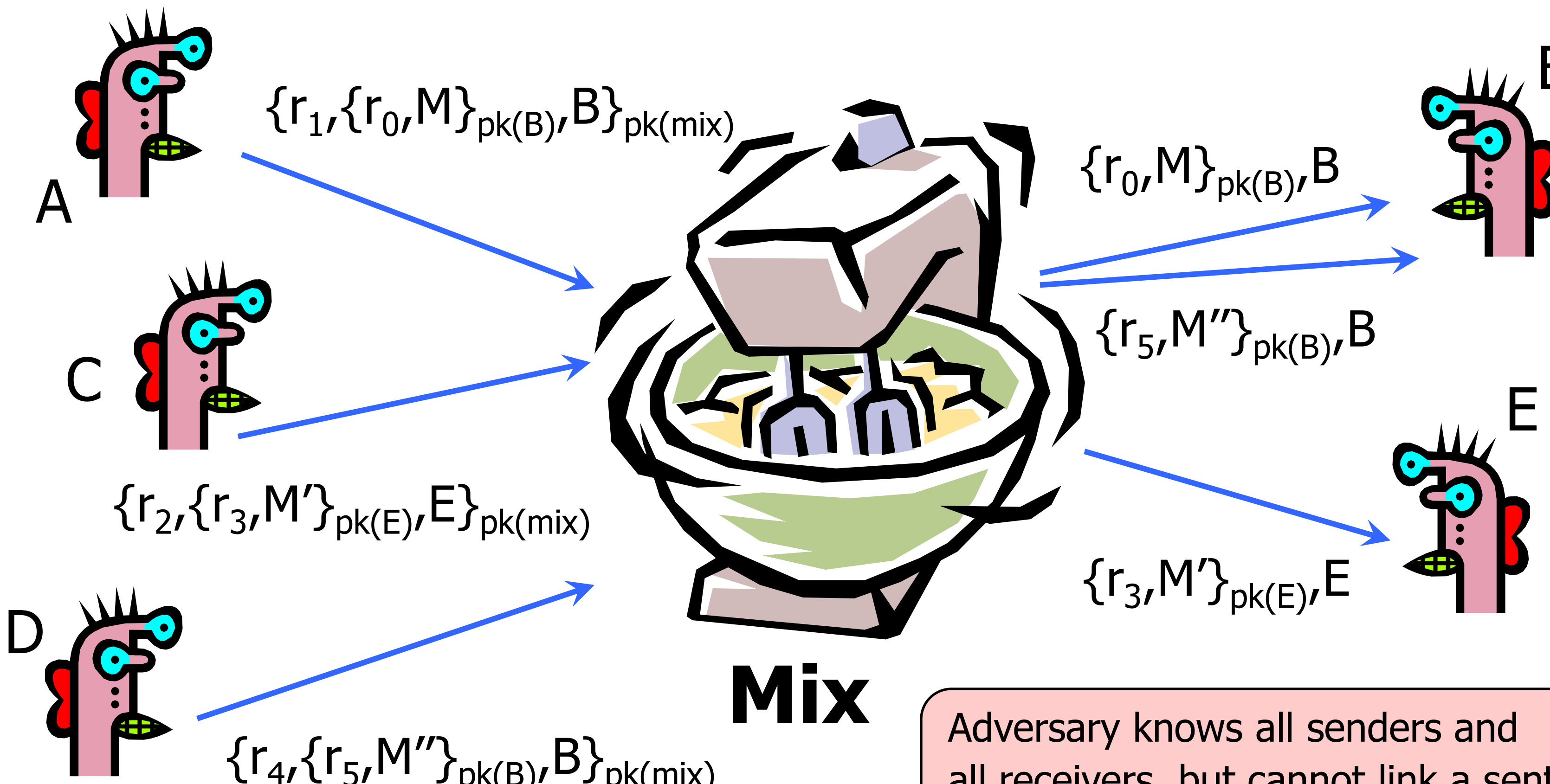
Chaum's Mix

- Early proposal for anonymous email
  - David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". Communications of the ACM, February 1981.

Before spam, people thought anonymous email was a good idea ☺

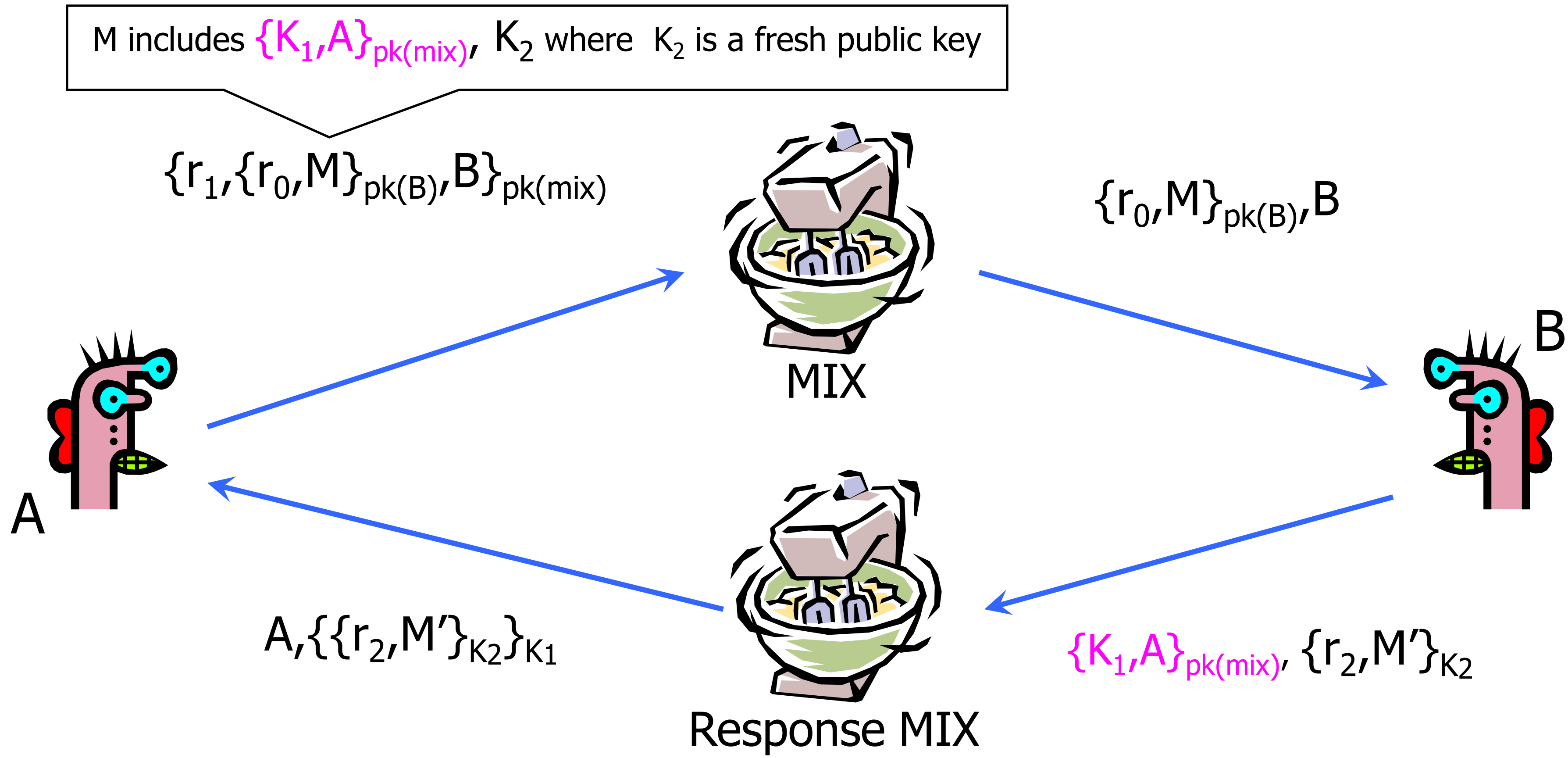
- Public key crypto + trusted re-mailer (Mix)
  - Untrusted communication medium
  - Public keys used as persistent pseudonyms
- Modern anonymity systems use Mix as the basic building block

Basic Mix Design



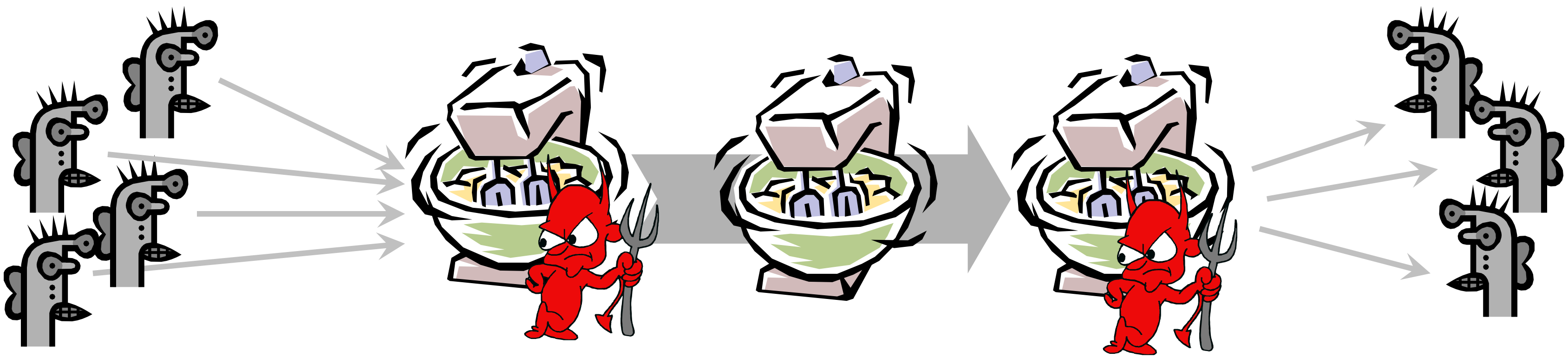
Adversary knows all senders and all receivers, but cannot link a sent message with a received message

Anonymous Return Addresses



Secrecy without authentication
(good for an online confession service ☺)

Mix Cascades and Mixnets



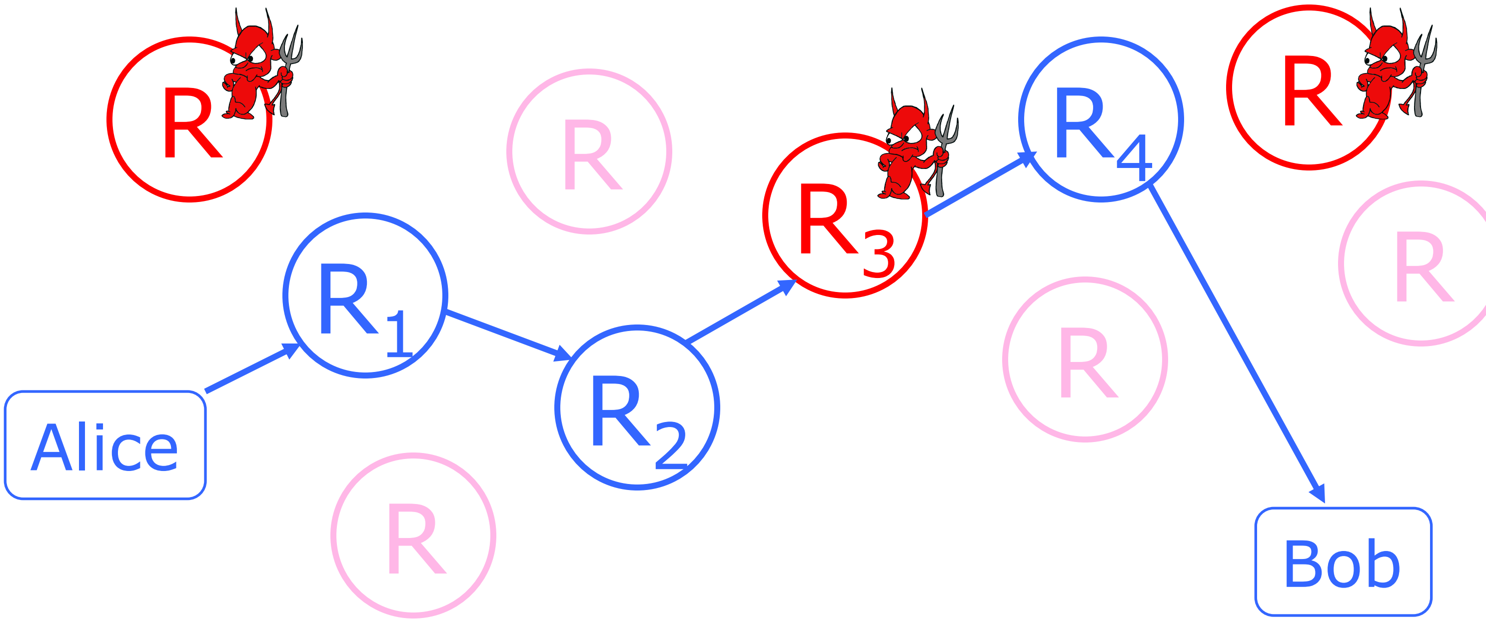
- Messages are sent through a sequence of mixes
  - Can also form an arbitrary network of mixes ("mixnet")
- Some of the mixes may be controlled by attacker, but even a single good mix ensures anonymity
- Pad and buffer traffic to foil correlation attacks

Disadvantages of Basic Mixnets

- Public-key encryption and decryption at each mix are computationally expensive
- Basic mixnets have high latency
  - Ok for email, but not for Web browsing
- Challenge: low-latency anonymity network
  - Use public-key cryptography to establish a “circuit” with pairwise symmetric keys between hops on the circuit
  - Then use symmetric decryption and re-encryption to move data messages along the established circuits
  - Each node behaves like a mix; anonymity is preserved even if some nodes are compromised

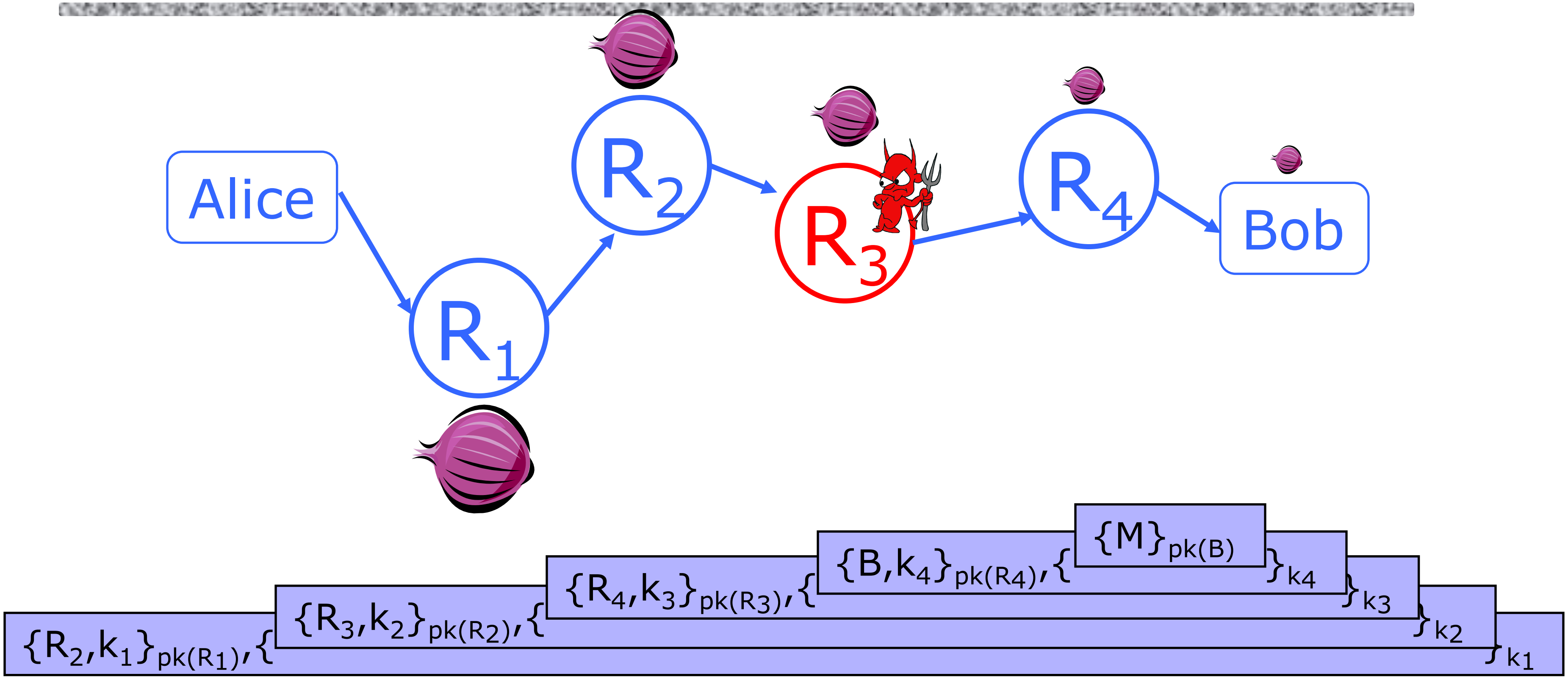
Onion Routing

[Reed, Syverson, Goldschlag 1997]



- Sender chooses a random sequence of routers
  - Some routers are honest, some controlled by attacker
  - Sender controls the length of the path

Route Establishment



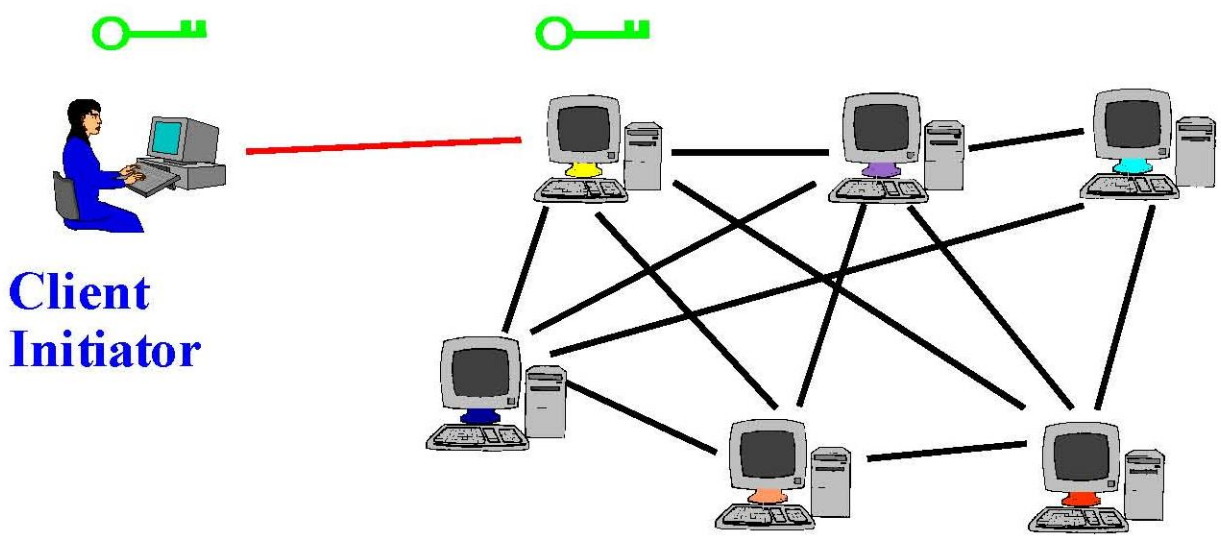
- Routing info for each link encrypted with router's public key
- Each router learns only the identity of the next router

Tor

- Second-generation onion routing network
  - http://tor.eff.org
  - Specifically designed for low-latency anonymous Internet communications (e.g., Web browsing)
  - Running since October 2003
- Hundreds of nodes on all continents
- Over 2,500,000 users
- “Easy-to-use” client
  - Freely available, can use it for anonymous browsing

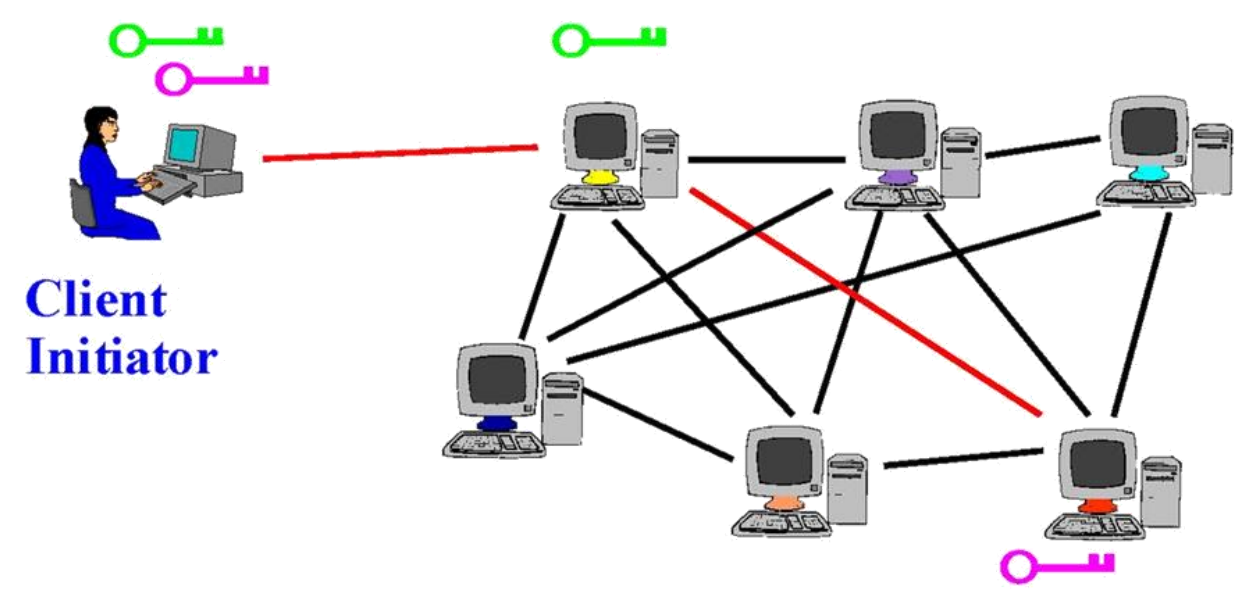
Tor Circuit Setup (1)

- Client proxy establishes a symmetric session key and circuit with Onion Router #1



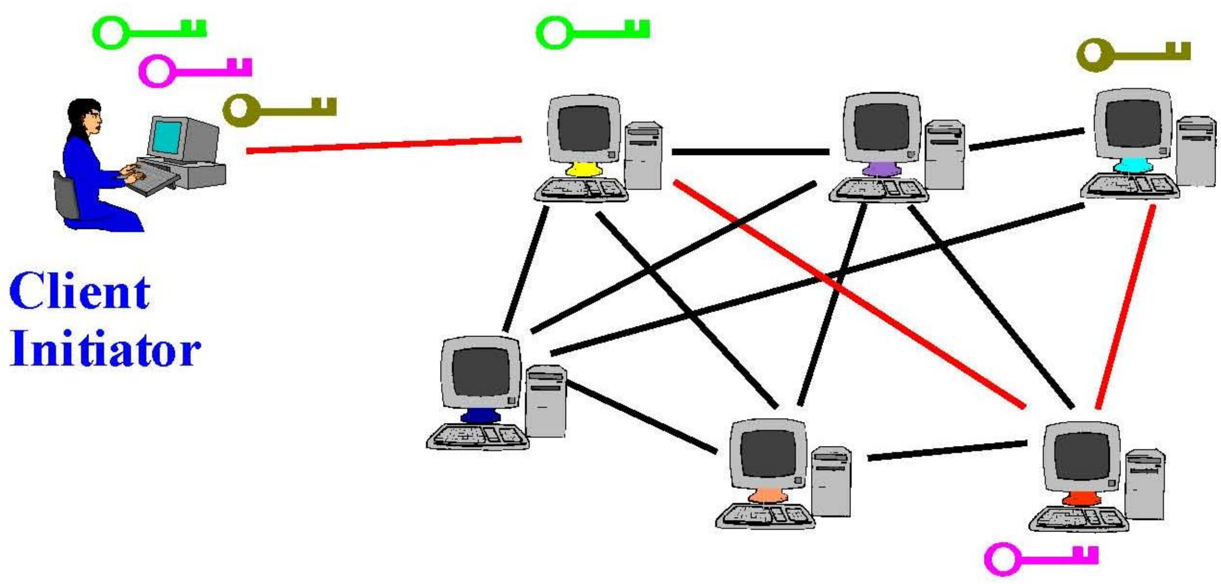
Tor Circuit Setup (2)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #2
  - Tunnel through Onion Router #1



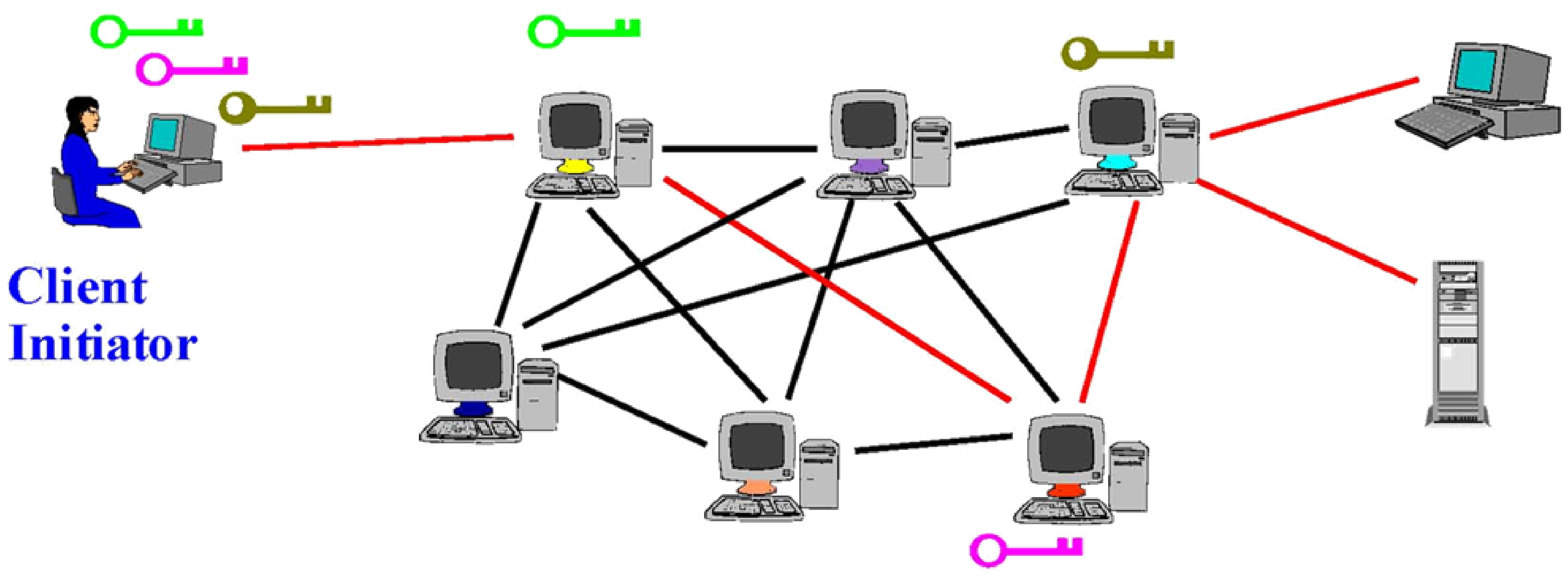
Tor Circuit Setup (3)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #3
  - Tunnel through Onion Routers #1 and #2



Using a Tor Circuit

- Client applications connect and communicate over the established Tor circuit
  - Datagrams are decrypted and re-encrypted at each link



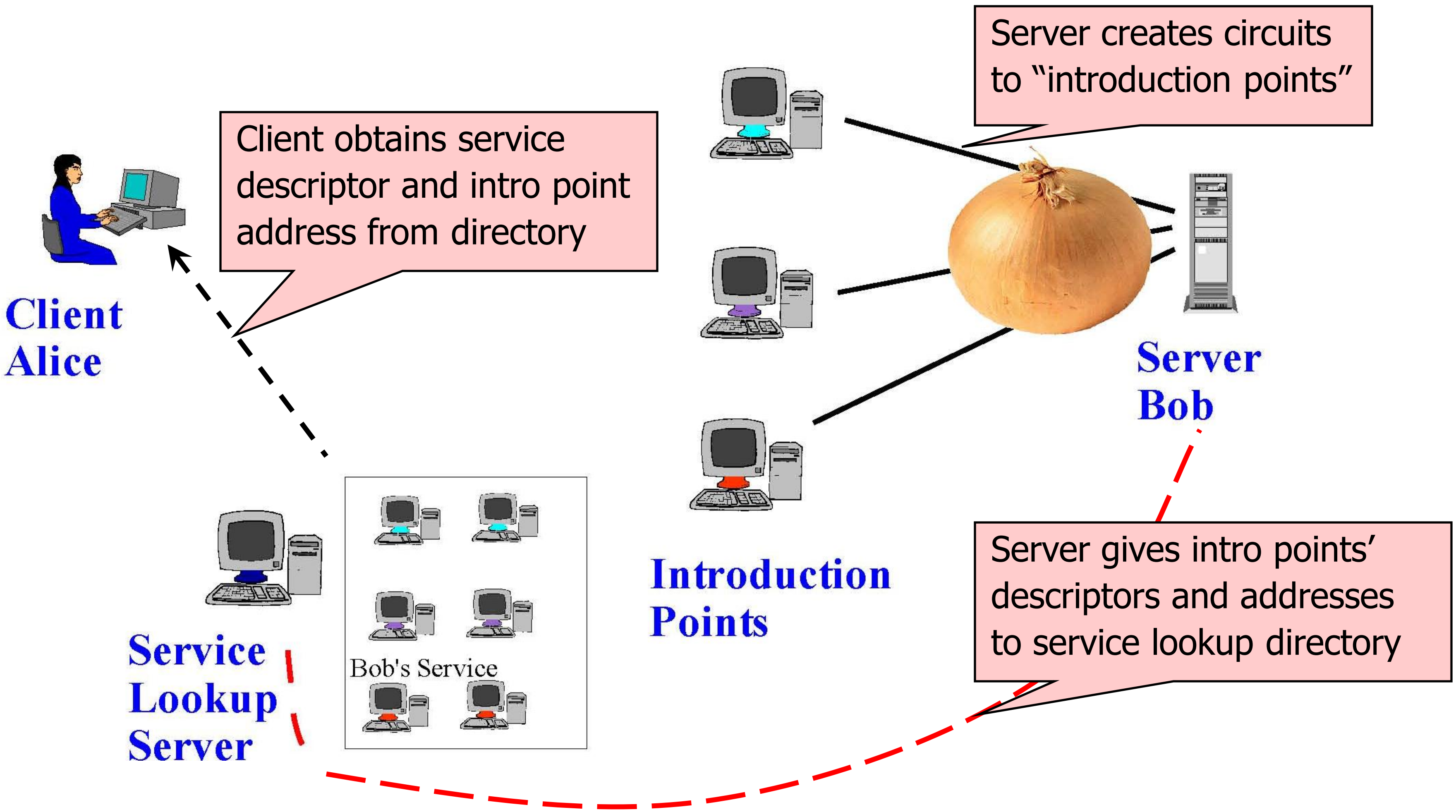
Tor Management Issues

- Many applications can share one circuit
  - Multiple TCP streams over one anonymous connection
- Tor router doesn't need root privileges
  - Encourages people to set up their own routers
  - More participants = better anonymity for everyone
- Directory servers
  - Maintain lists of active onion routers, their locations, current public keys, etc.
  - Control how new routers join the network
    - "Sybil attack": attacker creates a large number of routers
  - Directory servers' keys ship with Tor code

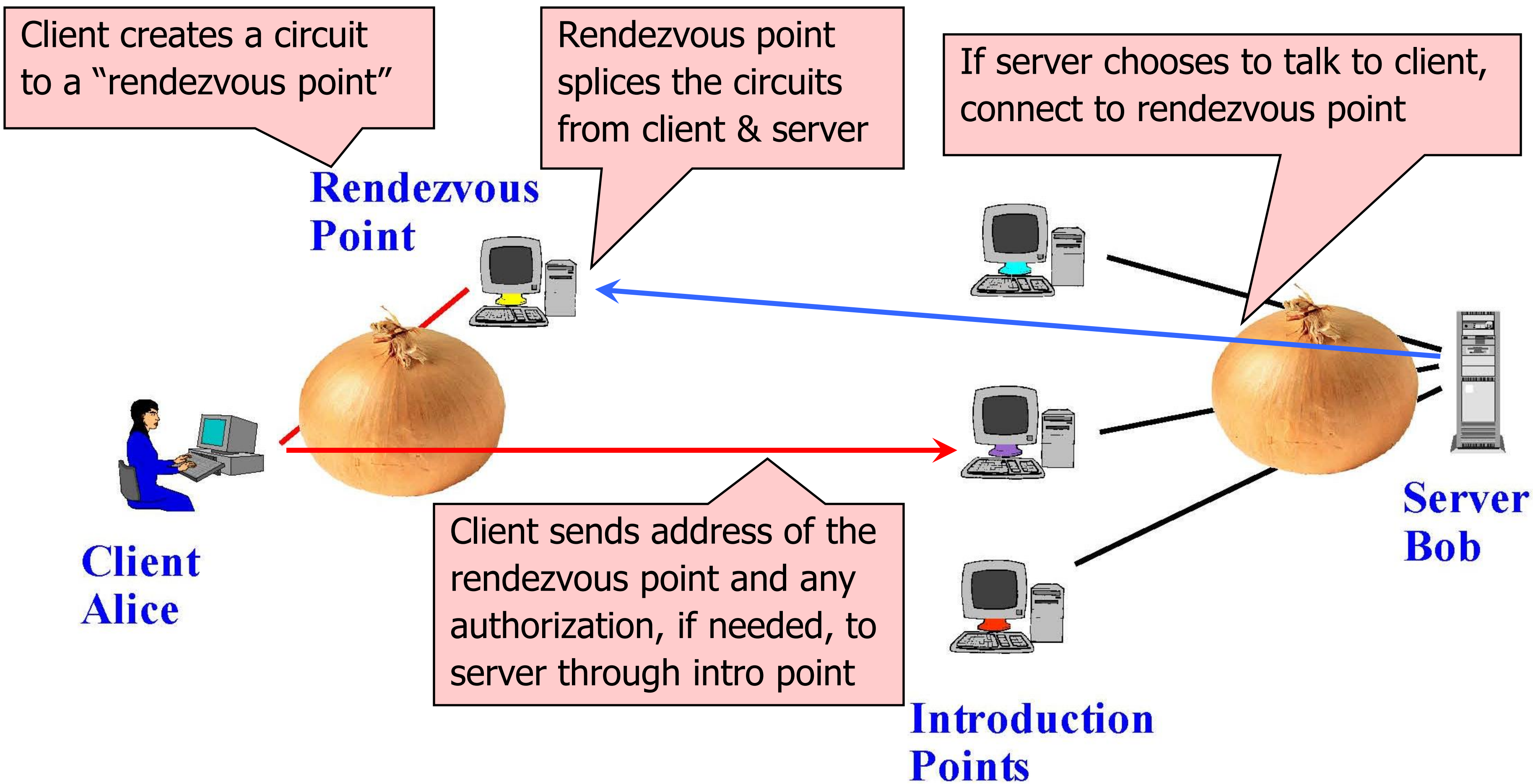
Location Hidden Services

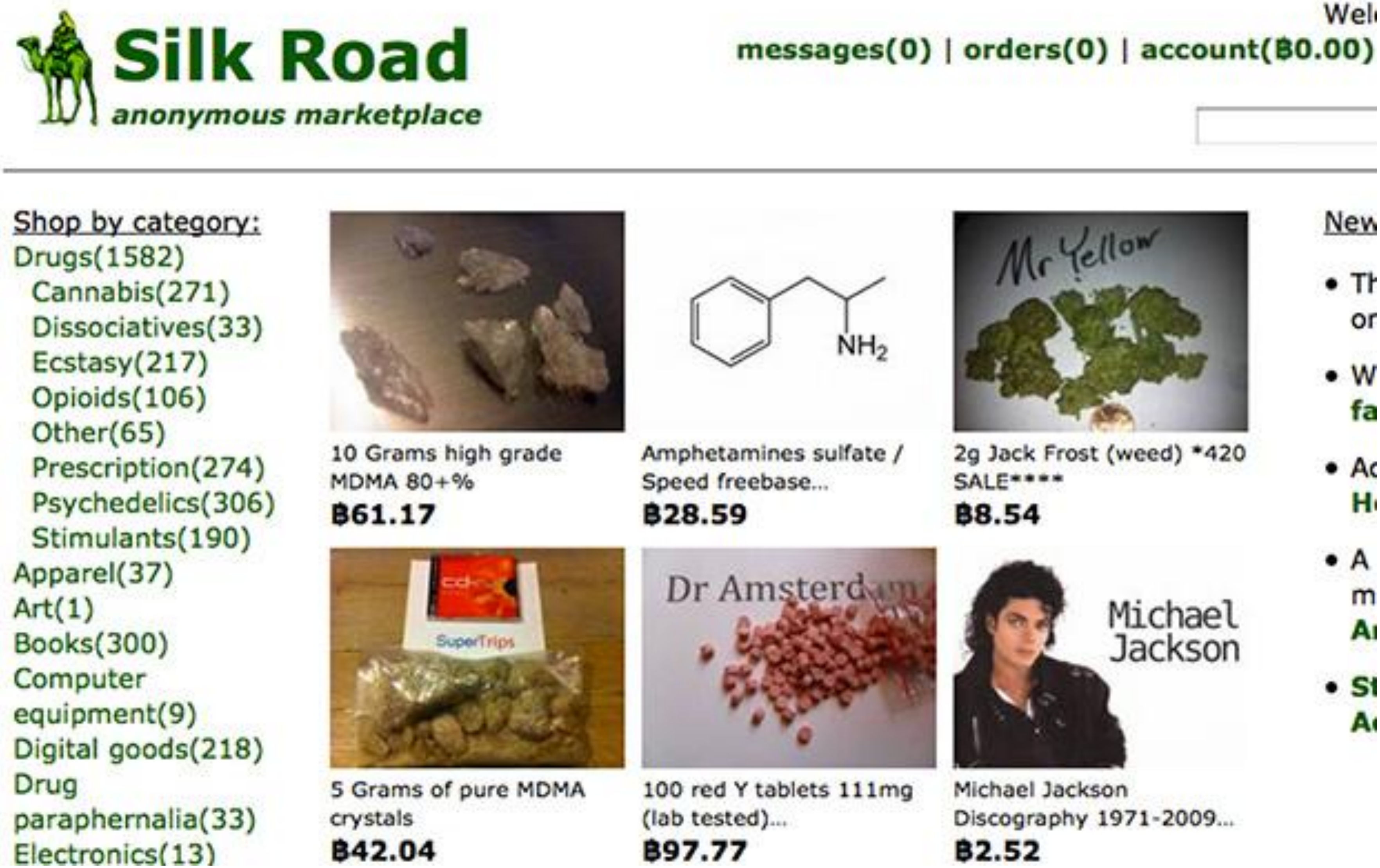
- Goal: deploy a server on the Internet that anyone can connect to without knowing where it is or who runs it
- Accessible from anywhere
- Resistant to censorship
- Can survive a full-blown DoS attack
- Resistant to physical attack
  - Can't find the physical server!

Creating a Location Hidden Server



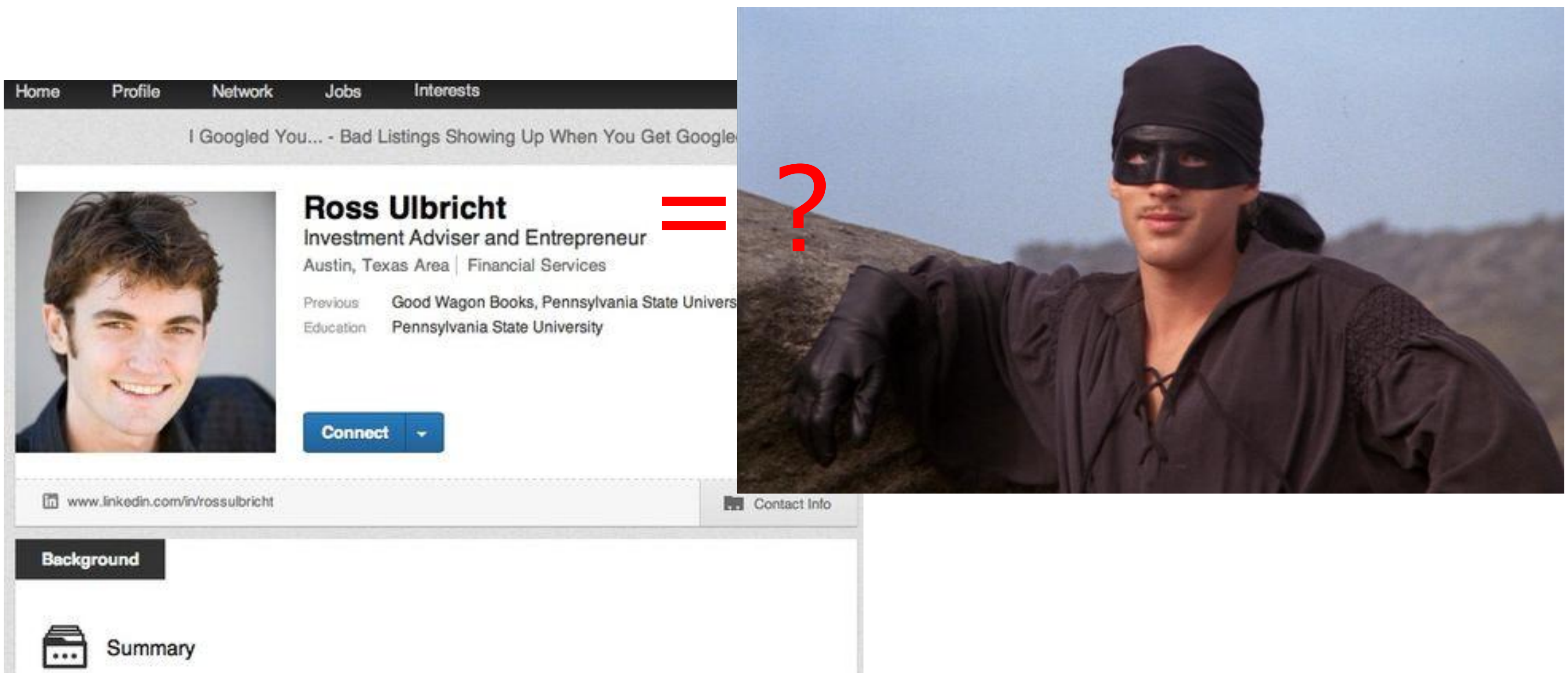
Using a Location Hidden Server




Silk Road
anonymous marketplace
messages(0) | orders(0) | account(฿0.00)
Shop by category:
Drugs(1582)
Cannabis(271)
Dissociatives(33)
Ecstasy(217)
Opioids(106)
Other(65)
Prescription(274)
Psychedelics(306)
Stimulants(190)
Apparel(37)
Art(1)
Books(300)
Computer equipment(9)
Digital goods(218)
Drug paraphernalia(33)
Electronics(13)
10 Grams high grade MDMA 80+%
฿61.17
NH2
Amphetamines sulfate / Speed freebase...
฿28.59
Mr Yellow
2g Jack Frost (weed) *420 SALE****
฿8.54
SuperTrips
5 Grams of pure MDMA crystals
฿42.04
Dr Amsterdam
100 red Y tablets 111mg (lab tested)...
฿97.77
Michael Jackson
Michael Jackson Discography 1971-2009...
฿2.52

Silk Road Shutdown

- Ross Ulbricht, alleged operator of the Silk Road Marketplace, arrested by the FBI on Oct 1, 2013



Silk Road Shutdown Theories

- A package of fake IDs from Canada traced to an apartment to San Francisco?
- A fake murder-for-hire arranged by DPR?
- A Stack Overflow question accidentally posted by Ulbricht under his real name?
  - "How can I connect to a Tor hidden service using curl in php?"
  - … a few seconds later, changed username to "frosty"
  - … oh, and the encryption key on the Silk Road server ends with the substring "frosty@frosty"
- Probably <u>not</u> weaknesses in Tor

Dining Cryptographers

- Clever idea how to make a message public in a perfectly untraceable manner
  - David Chaum. "The dining cryptographers problem: unconditional sender and recipient untraceability." Journal of Cryptology, 1988.
- Guarantees information-theoretic anonymity for message senders
  - This is an unusually strong form of security: defeats adversary who has <u>unlimited</u> computational power
- Difficult to make practical
  - In a group of size N, need N random bits to send 1 bit

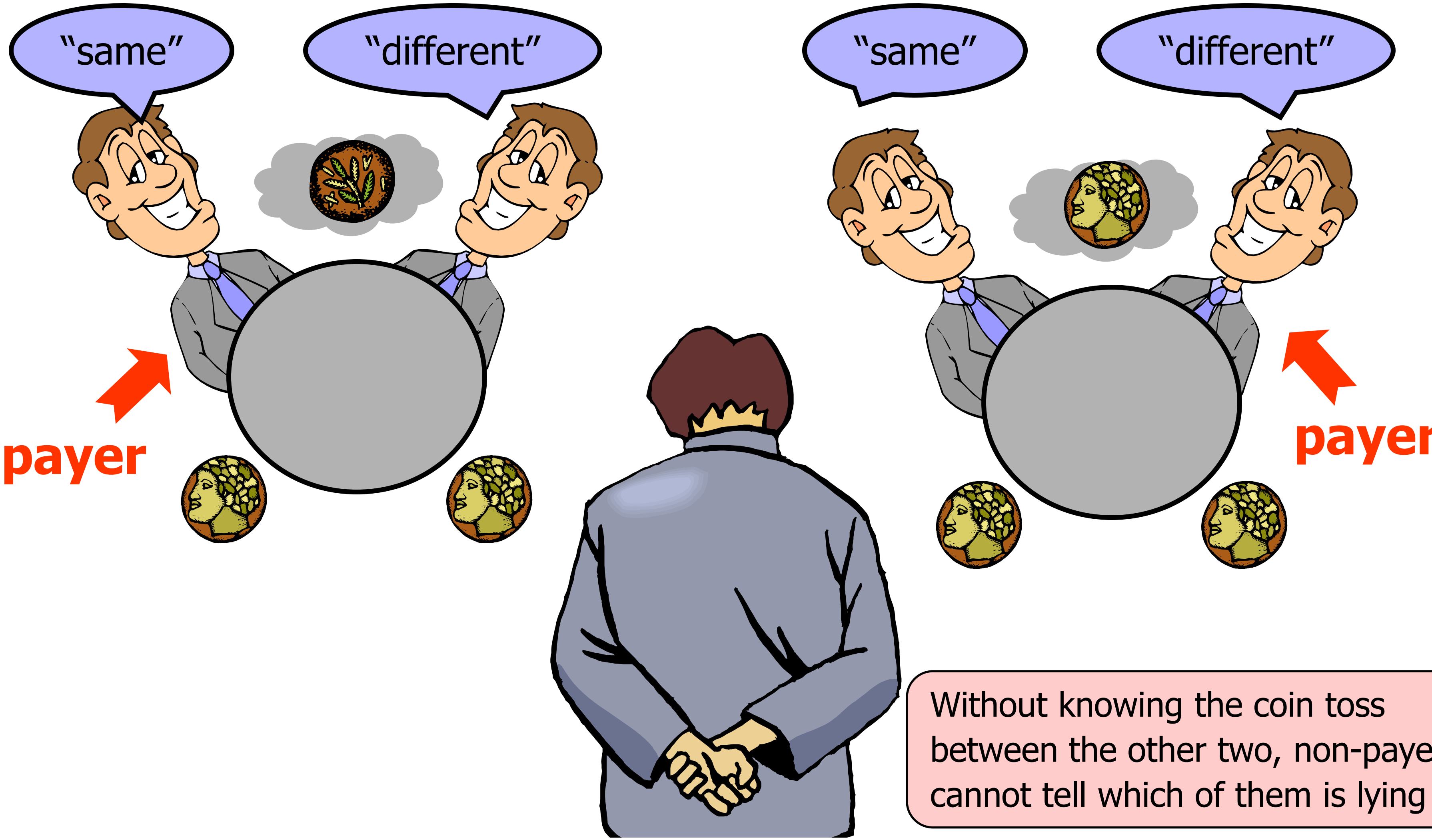
Three-Person DC Protocol

Three cryptographers are having dinner.
Either NSA is paying for the dinner, or
one of them is paying, but wishes to remain anonymous.

1. Each diner flips a coin and shows it to his left neighbor
   - Every diner will see two coins: his own and his right neighbor's
2. Each diner announces whether the two coins are the same; if he is the payer, he lies (says the opposite)
3. Odd number of "same" $\Rightarrow$ NSA is paying

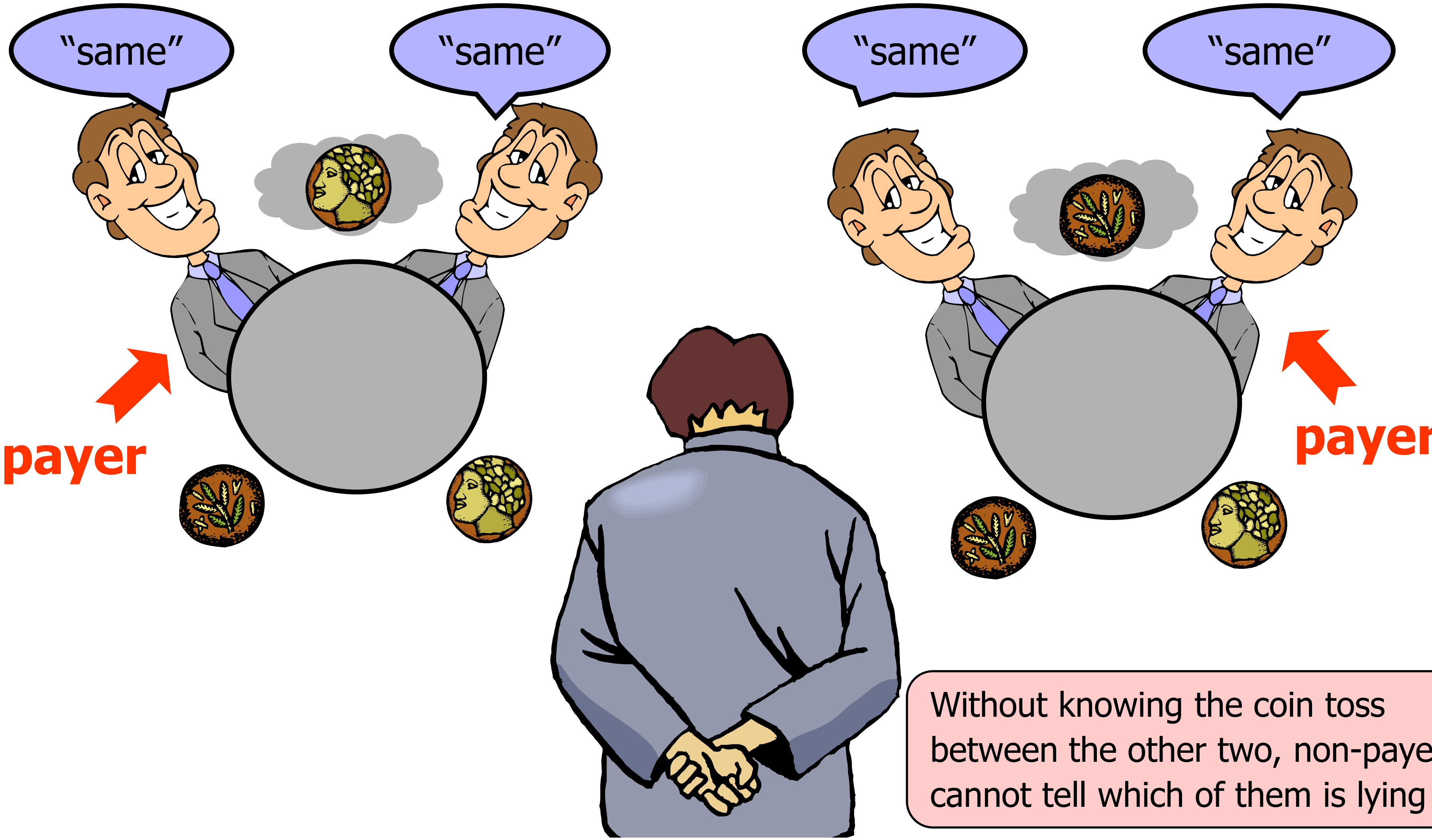
   Even number of "same" $\Rightarrow$ one of them is paying
   - But a non-payer cannot tell which of the other two is paying!

Non-Payer's View: Same Coins



Without knowing the coin toss between the other two, non-payer cannot tell which of them is lying

Non-Payer's View: Different Coins



Without knowing the coin toss between the other two, non-payer cannot tell which of them is lying

Superposed Sending

- This idea generalizes to any group of size N
- For each bit of the message, every user generates 1 random bit and sends it to 1 neighbor
  - Every user learns 2 bits (his own and his neighbor's)
- Each user announces (own bit XOR neighbor's bit)
- Sender announces (own bit XOR neighbor's bit XOR message bit)
- XOR of all announcements = message bit
  - Every randomly generated bit occurs in this sum twice (and is canceled by XOR), message bit occurs once