Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms

EJ Jung

usfCS UNIVERSITY of SAN FRANCISCO department of computer science

Goals

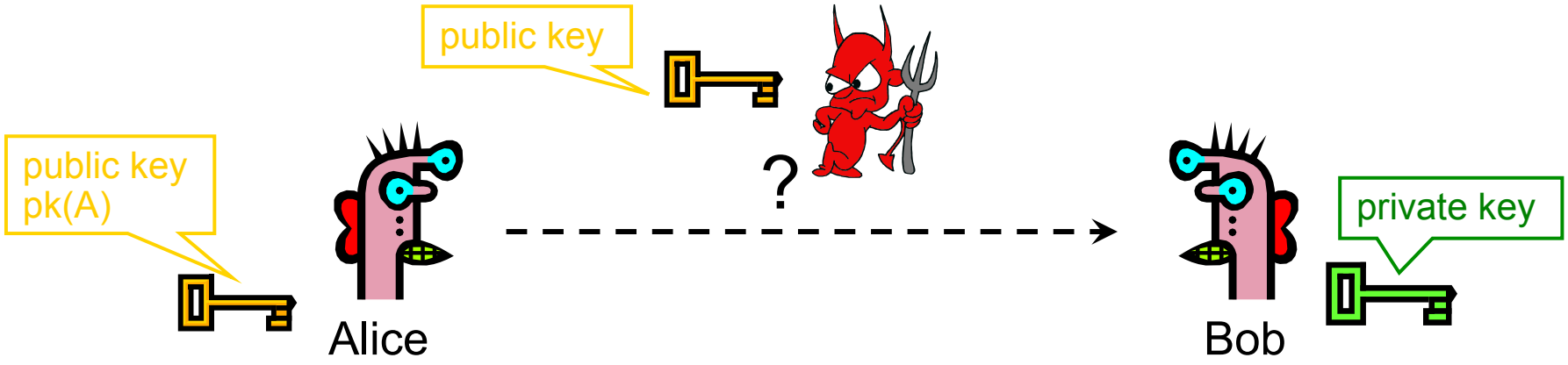
1. Hide what you wrote
   - encryption of any kind
   - symmetric/asymmetric/stream
2. Hide to whom you sent and when
   - pseudonym? proxy?
   - traffic analysis problem
3. Still receive a reply
   - hidden return address

usfCS UNIVERSITY of SAN FRANCISCO department of computer science

Despite..

- No trusted authority
  - cannot send the mail to this and ask to forward
- Insecure underlying communication
  - cannot send the mail over "hot channel"
  - attacker can eavesdrop any message on any link
  - attacker can inject/modify/record any messeges

Good news(?)

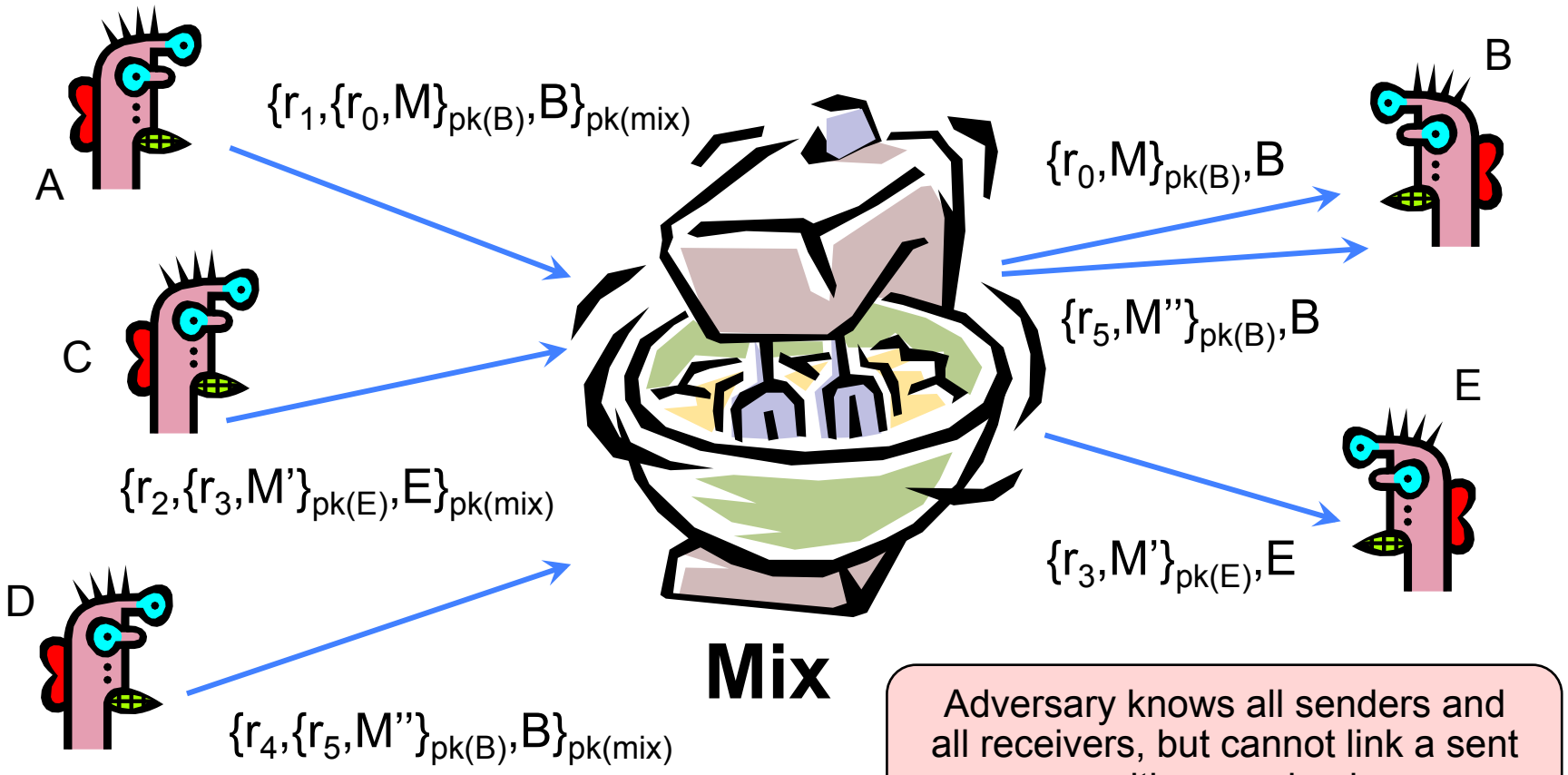


Given: Everybody knows Bob's public key

Only Bob knows the corresponding private key

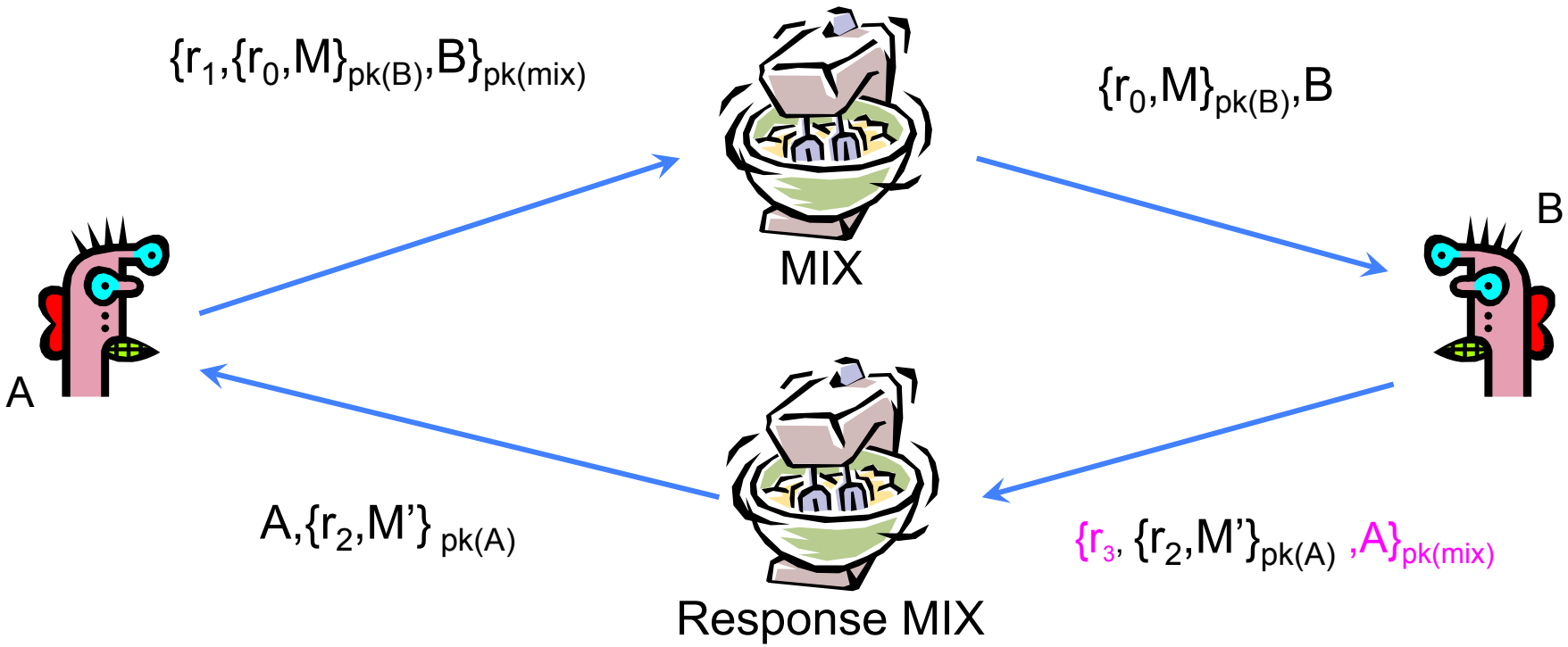
Assumptions: 1. Attacker cannot guess the private key based on public key
2. Attacker cannot convince Alice a wrong public key of Bob
- How to achieve this in real world?

Basic Mix Design



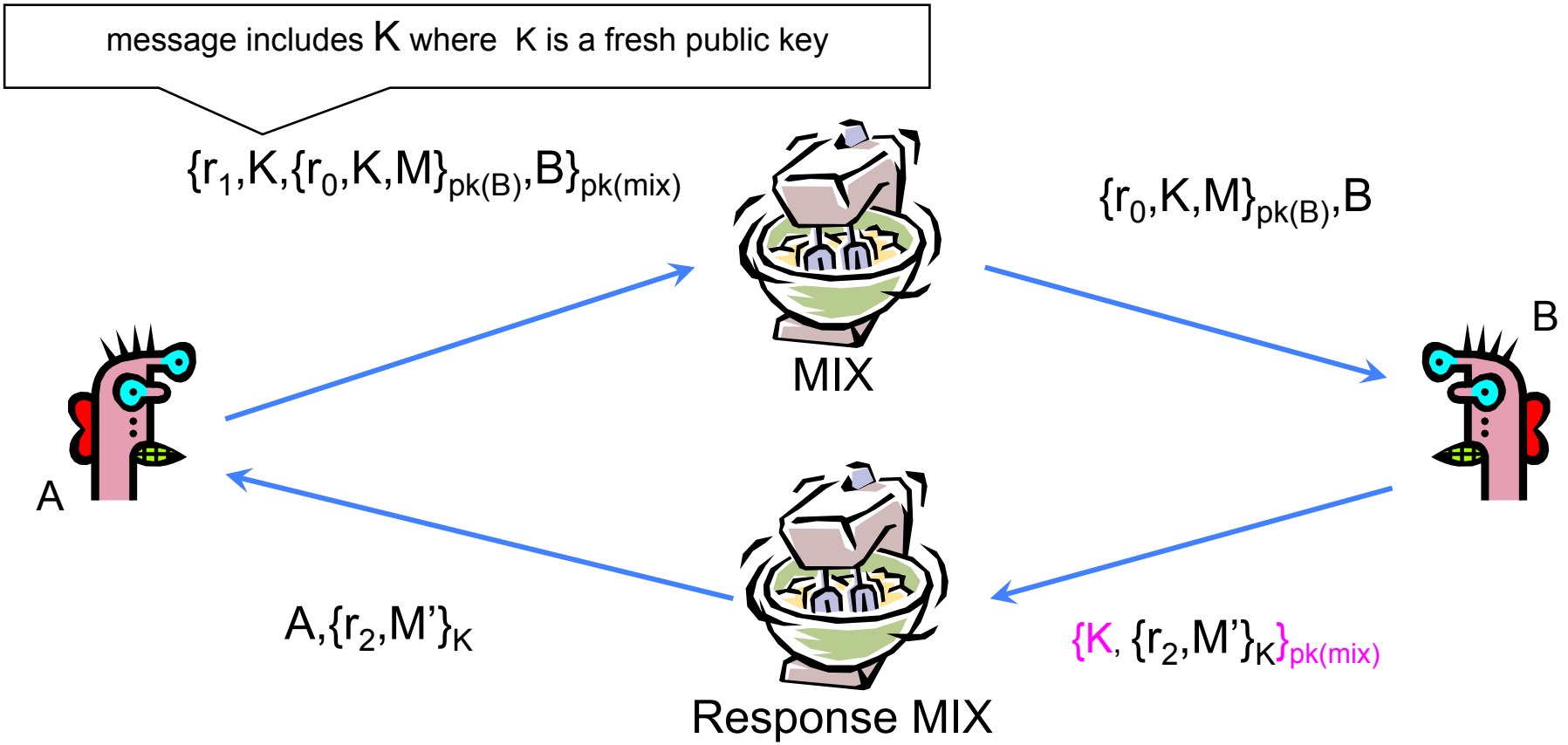
Adversary knows all senders and all receivers, but cannot link a sent message with a received message

Anonymous Return Address (0)



What's wrong with this?
- B knows who A is!

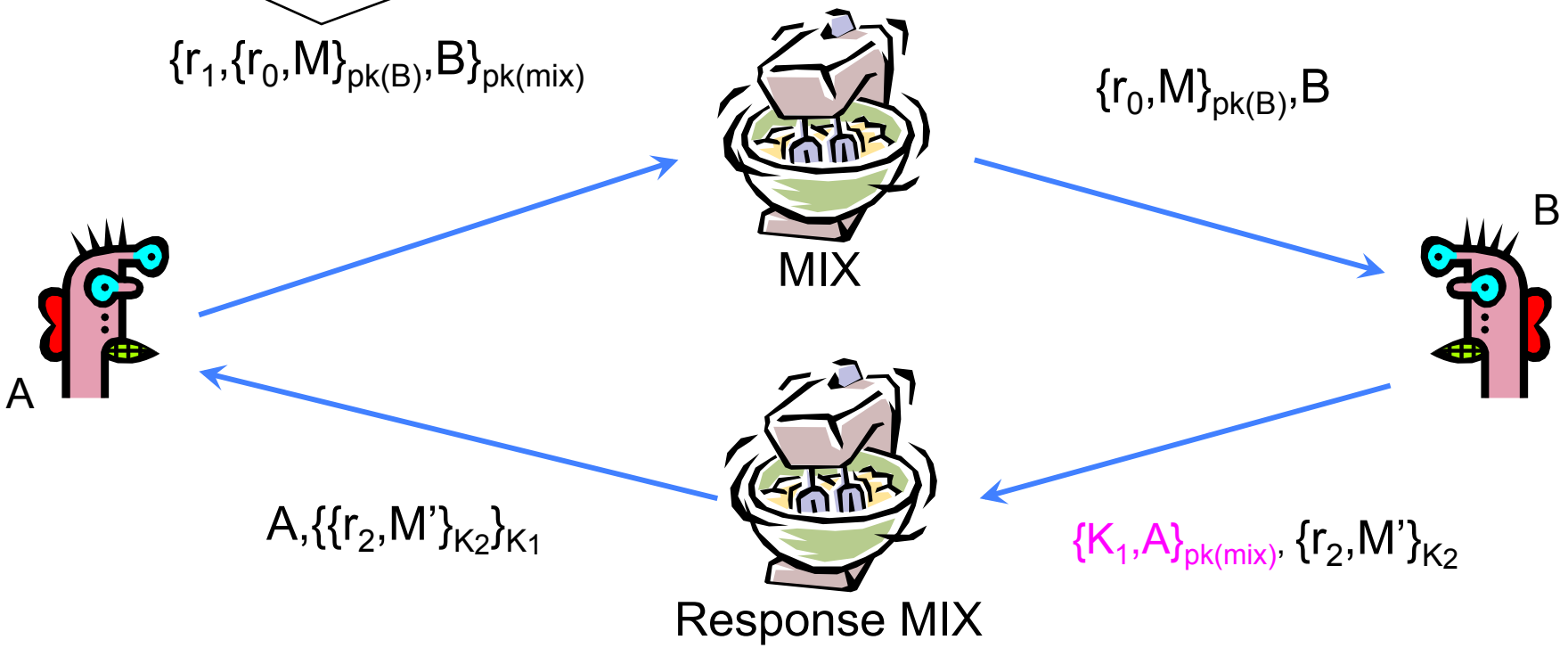
Anonymous Return Address (1)



Anonymous Return Address (2)

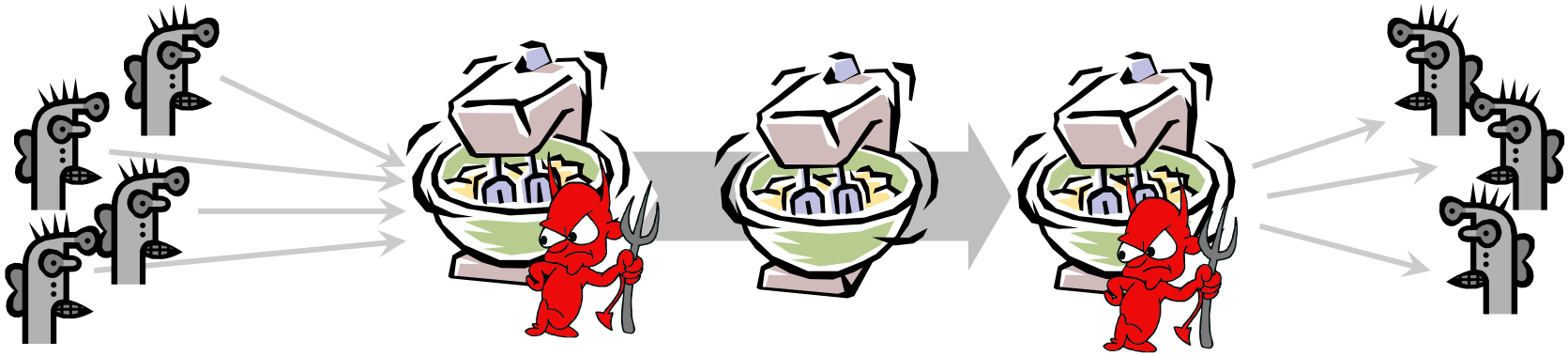
Q: Why A needs to encrypt $\{K_1,A\}_{pk(mix)}$, not B?

M includes $\{K_1,A\}_{pk(mix)}$, K_2 where K_2 is a fresh public key



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

Mix Cascade



- 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 guarantees anonymity
- Pad and buffer traffic to foil correlation attacks

usfCS
UNIVERSITY of SAN FRANCISCO
department of computer science

Small tricks

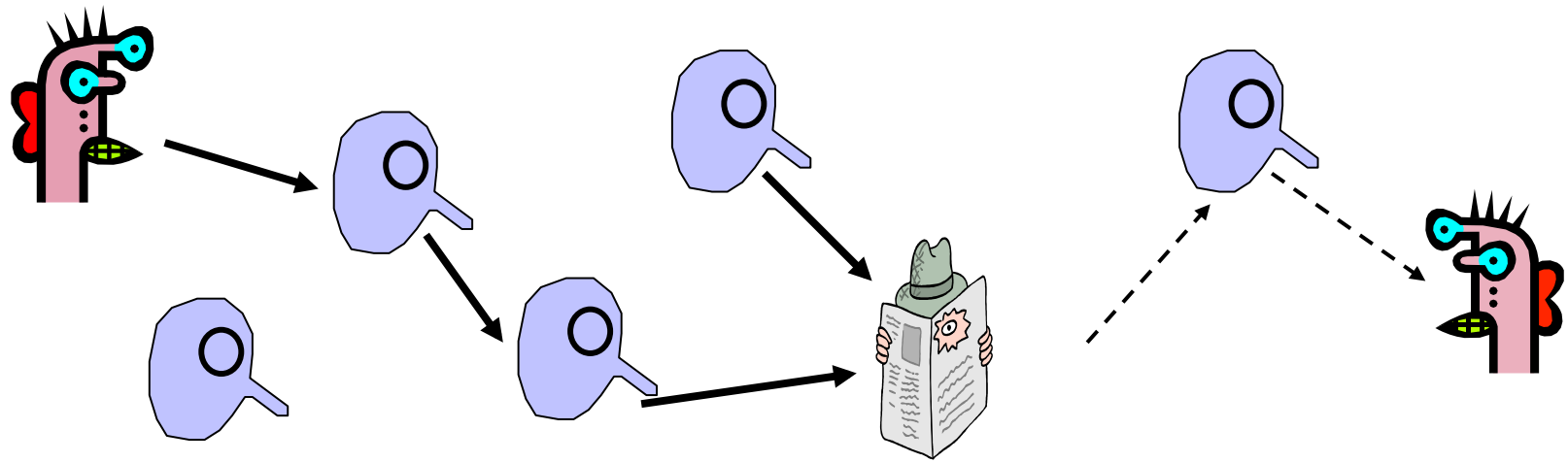
- Size-based correlation
  - send in fixed size blocks
- Timing-based correlation
  - send a random string even in idle times
- Frequency-based correlation
  - send always at maximum rate

usfCS UNIVERSITY of SAN FRANCISCO department of computer science

Disadvantages of Basic Mixnets

- Public-key encryption and decryption at each mix are computationally expensive
- Basic mixnets have high latency
  - Ok for email, not Ok for anonymous 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

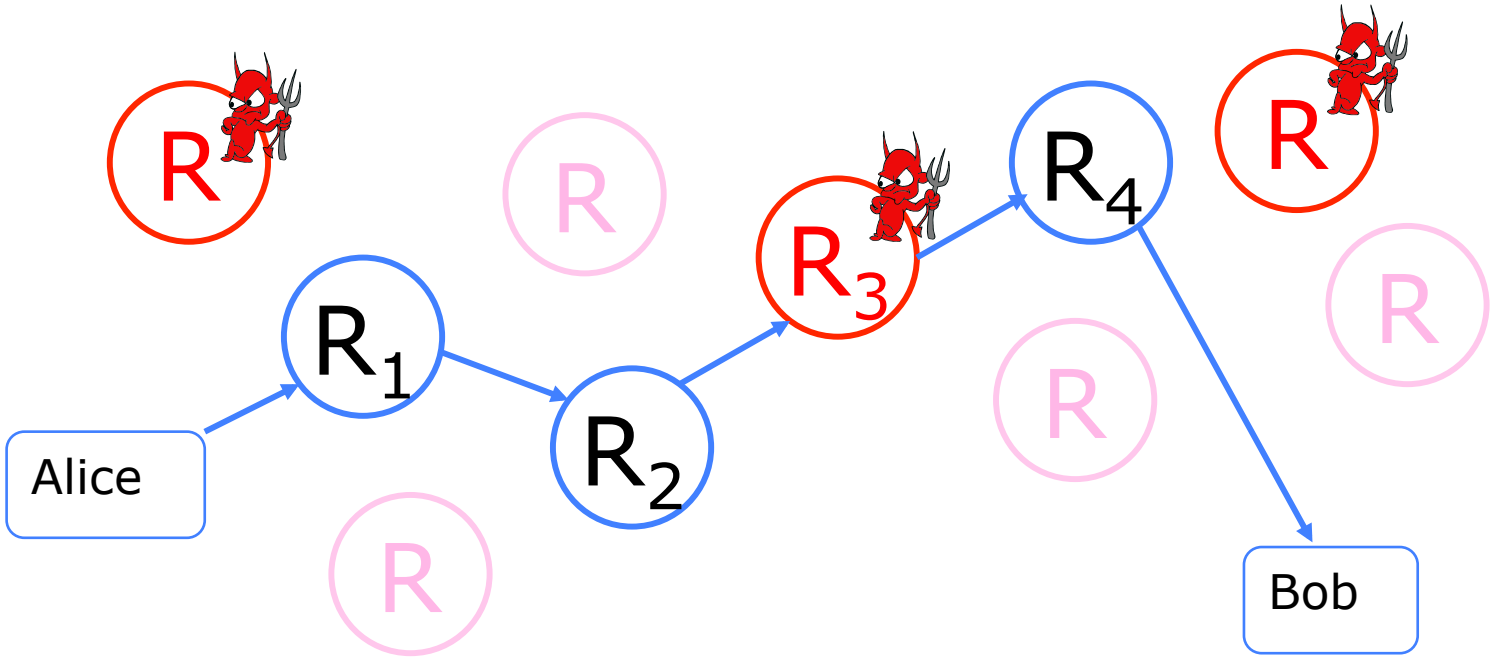
Another Idea: Randomized Routing



- Hide message source by routing it randomly
  - Popular technique: Crowds, Freenet, Onion routing
- Routers don't know for sure if the apparent source of a message is the true sender or another router

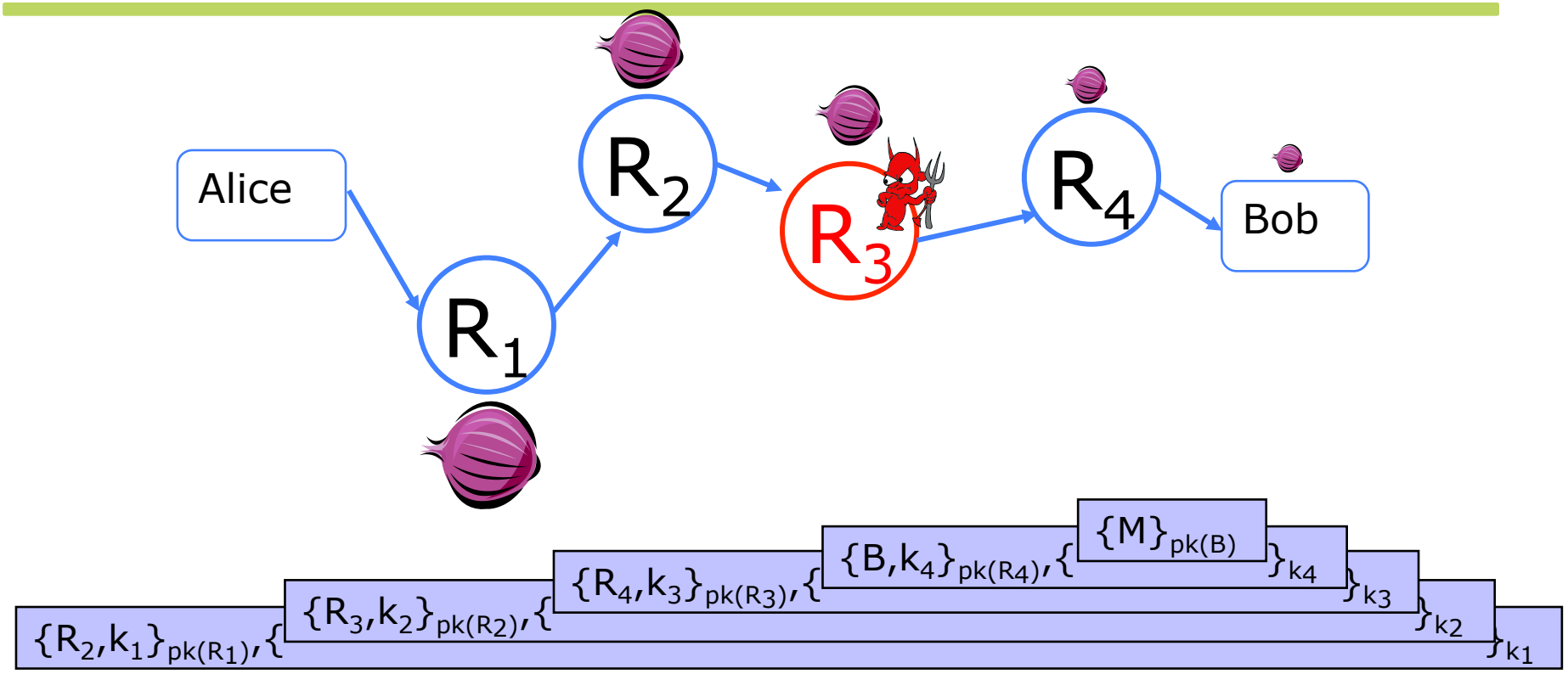
Onion Routing

[Reed, Syverson, Goldschlag '97]



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

Route Establishment

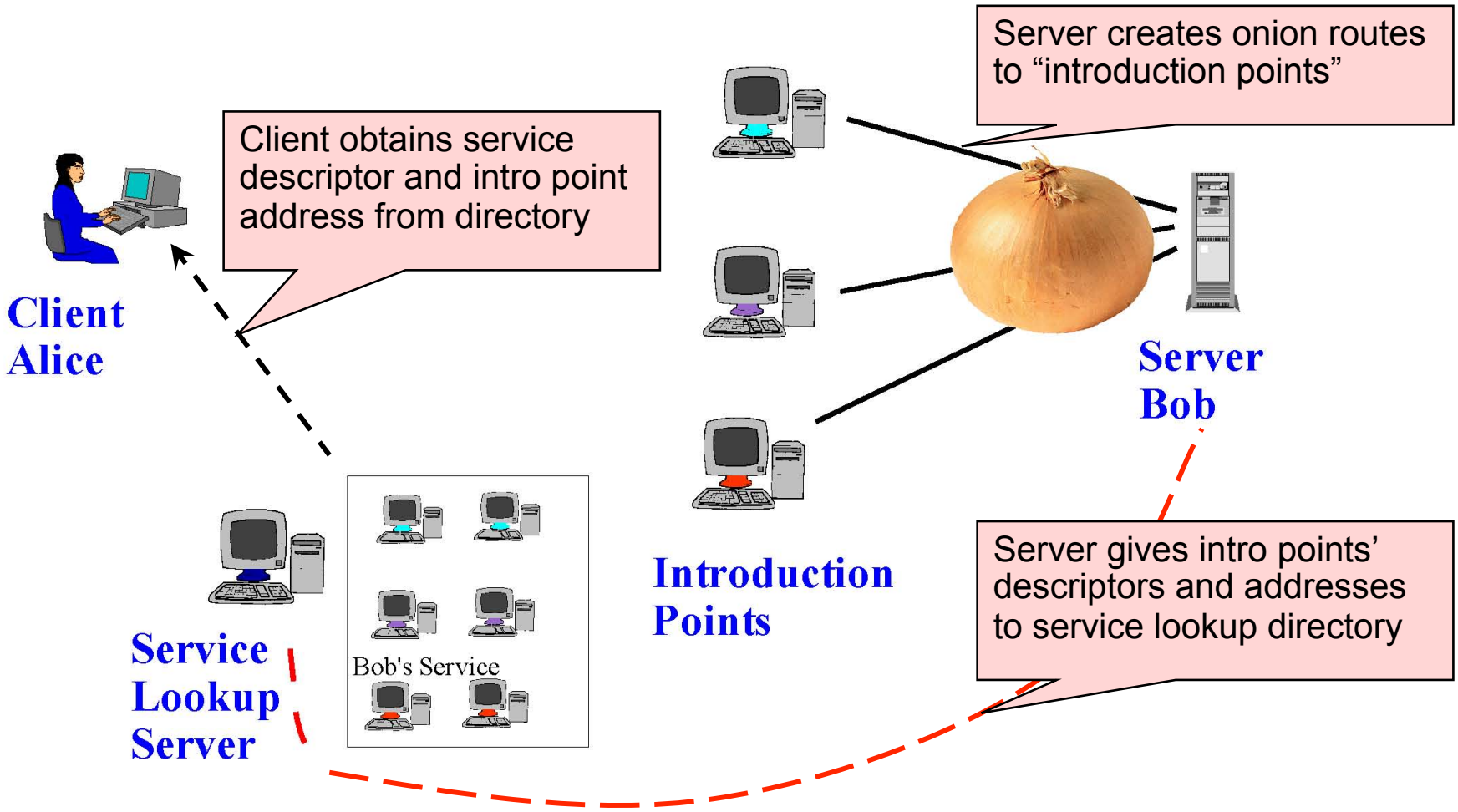


Routing info for each link encrypted with router's public key
Each router learns only the identity of the next router

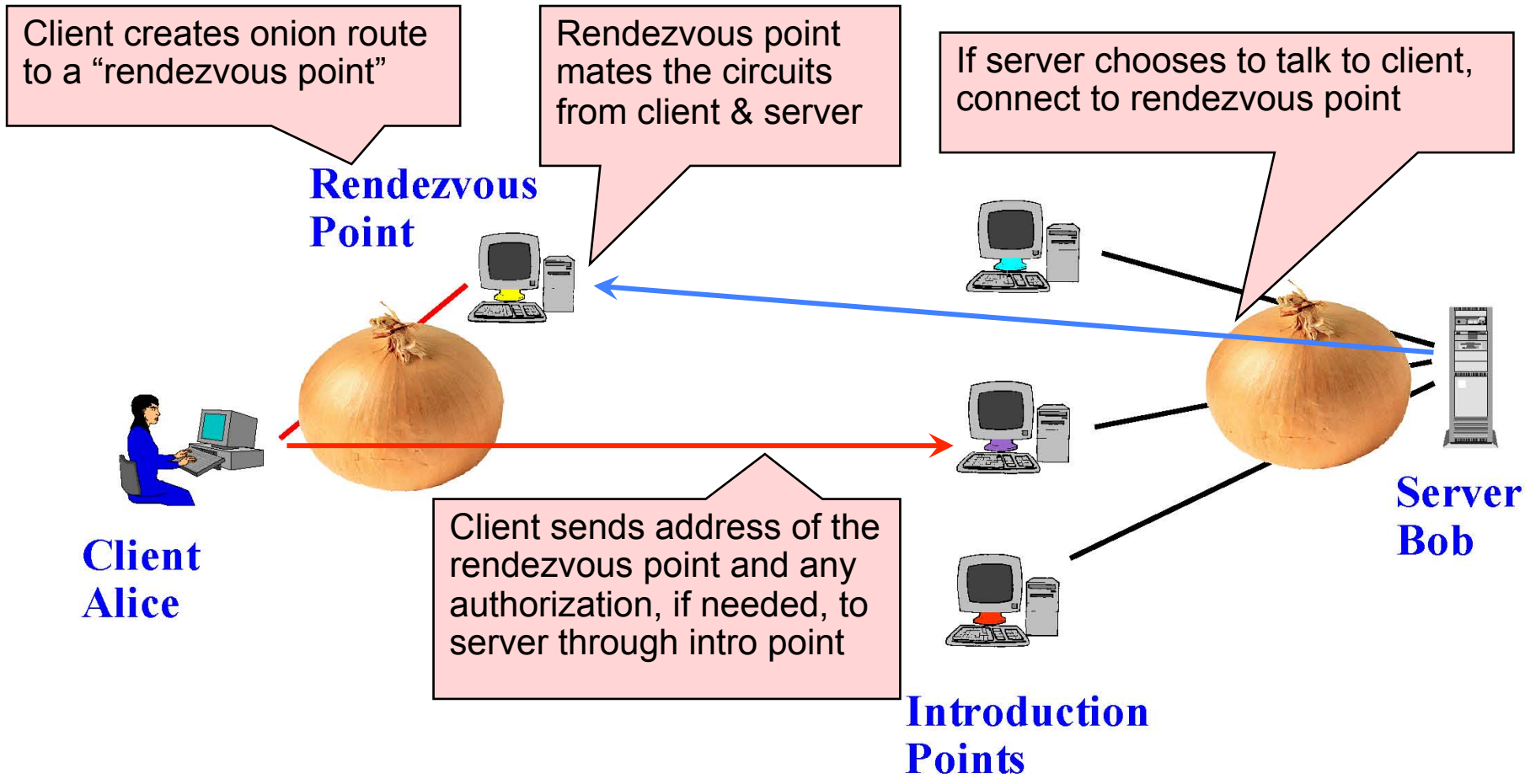
Location Hidden Servers

- 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 full-blown DoS attack
- Resistant to physical attack
  - Can't find the physical server!

Creating a Location Hidden Server



Using a Location Hidden Server



Deployed Anonymity Systems

- Free Haven project has an excellent bibliography on anonymity
  - http://freehaven.net/anonbib/date.html
- TOR (http://www.torproject.org/)
  - Overlay circuit-based anonymity network
  - Best for low-latency applications such as anonymous Web browsing
- Mixminion (http://www.mixminion.net)
  - Network of mixes
  - Designed for high-latency applications such as anonymous email