Anonymous Communication with emphasis on Tor*

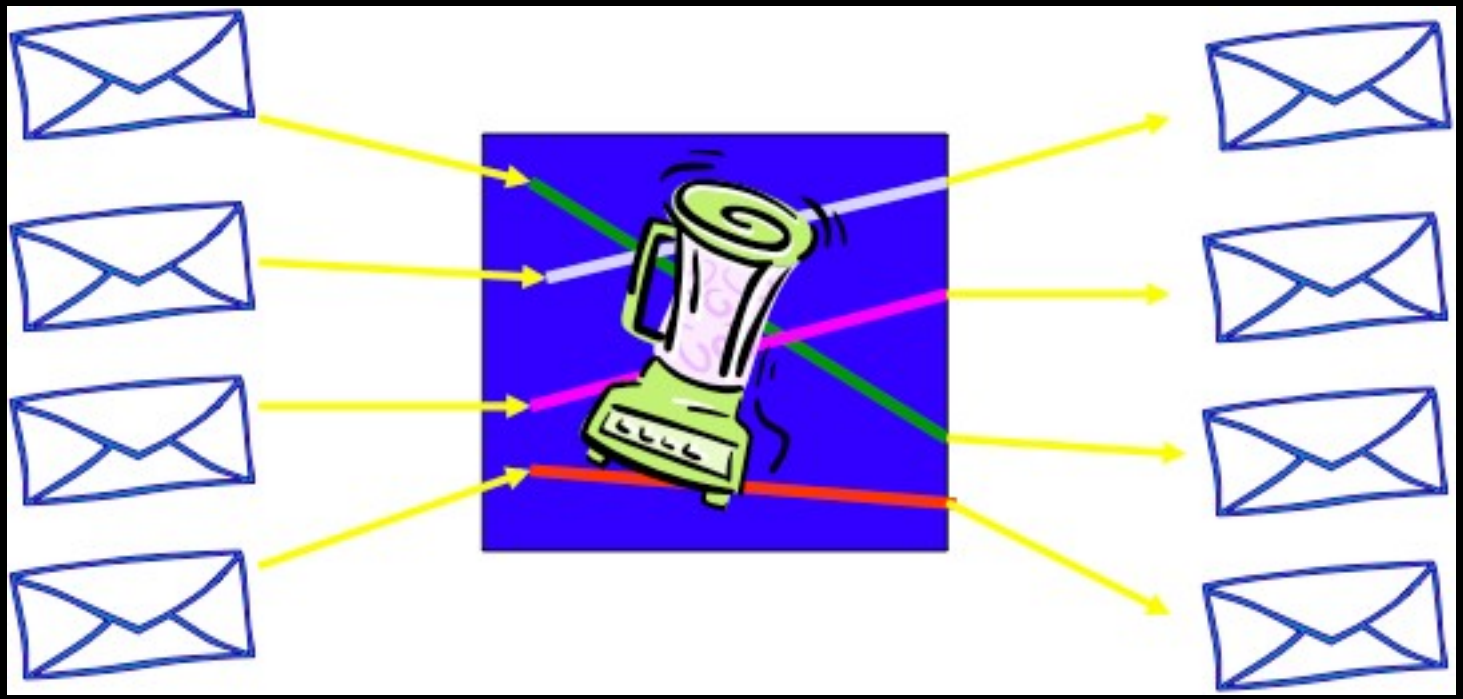
*Tor's Onion Routing

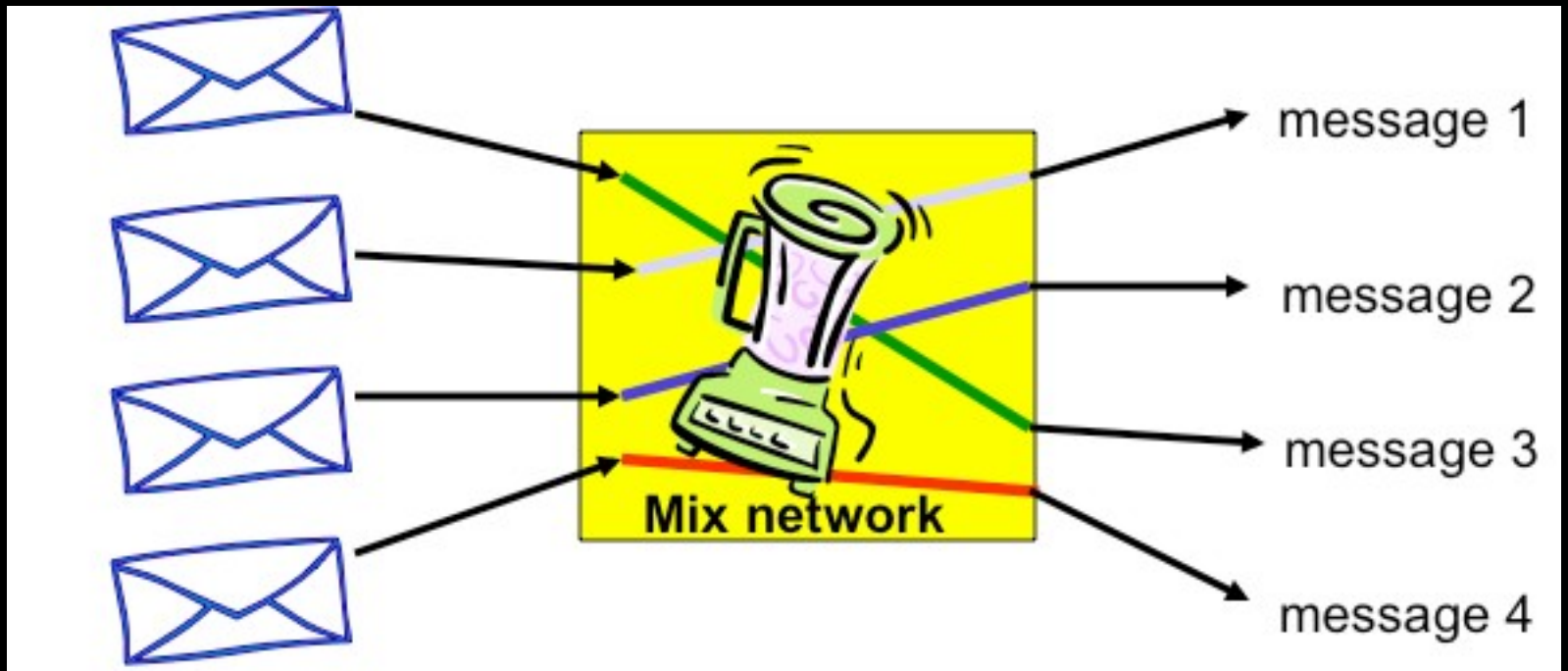
Paul Syverson
U.S. Naval Research Laboratory

Dining Cryptographers (DC Nets)

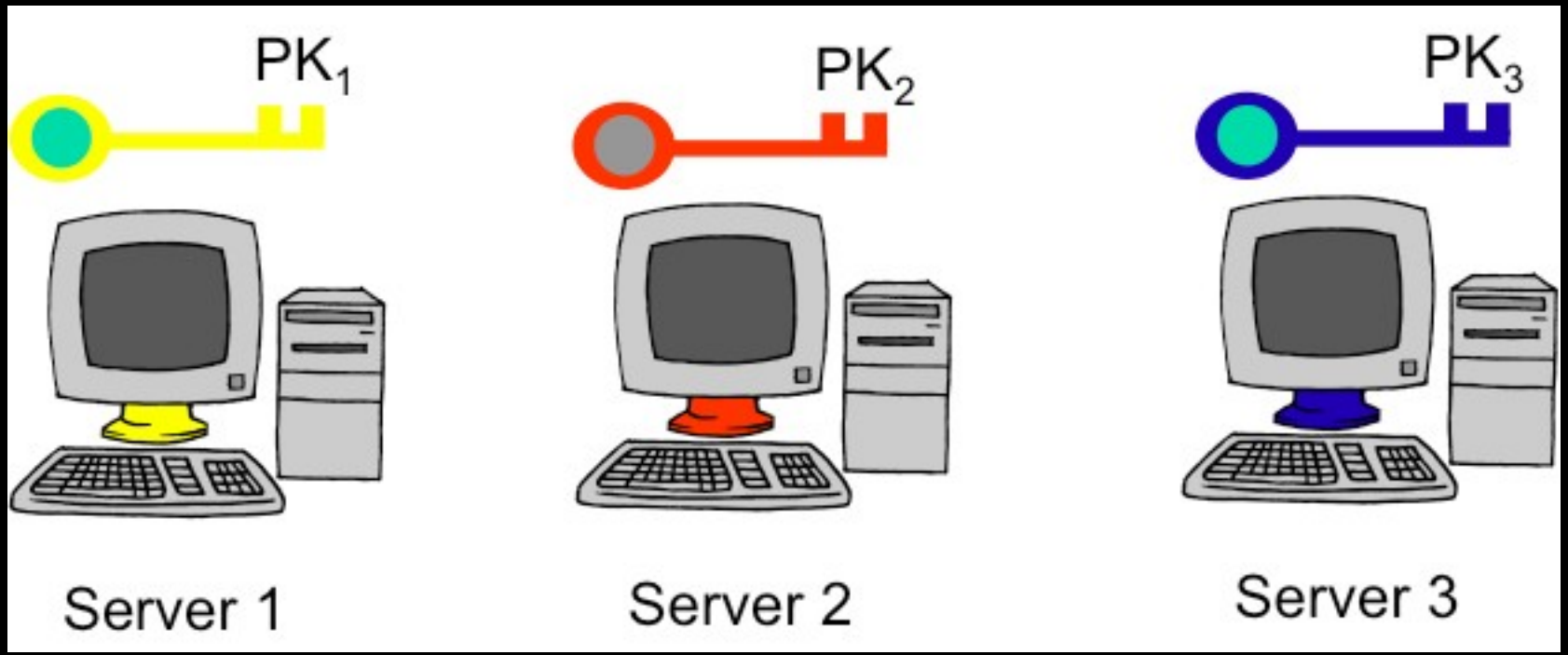
- Invented by Chaum, 1988
- Strong provable properties
- Versions without collision or abuse problems have high communication and computation overhead
- Don't scale very well

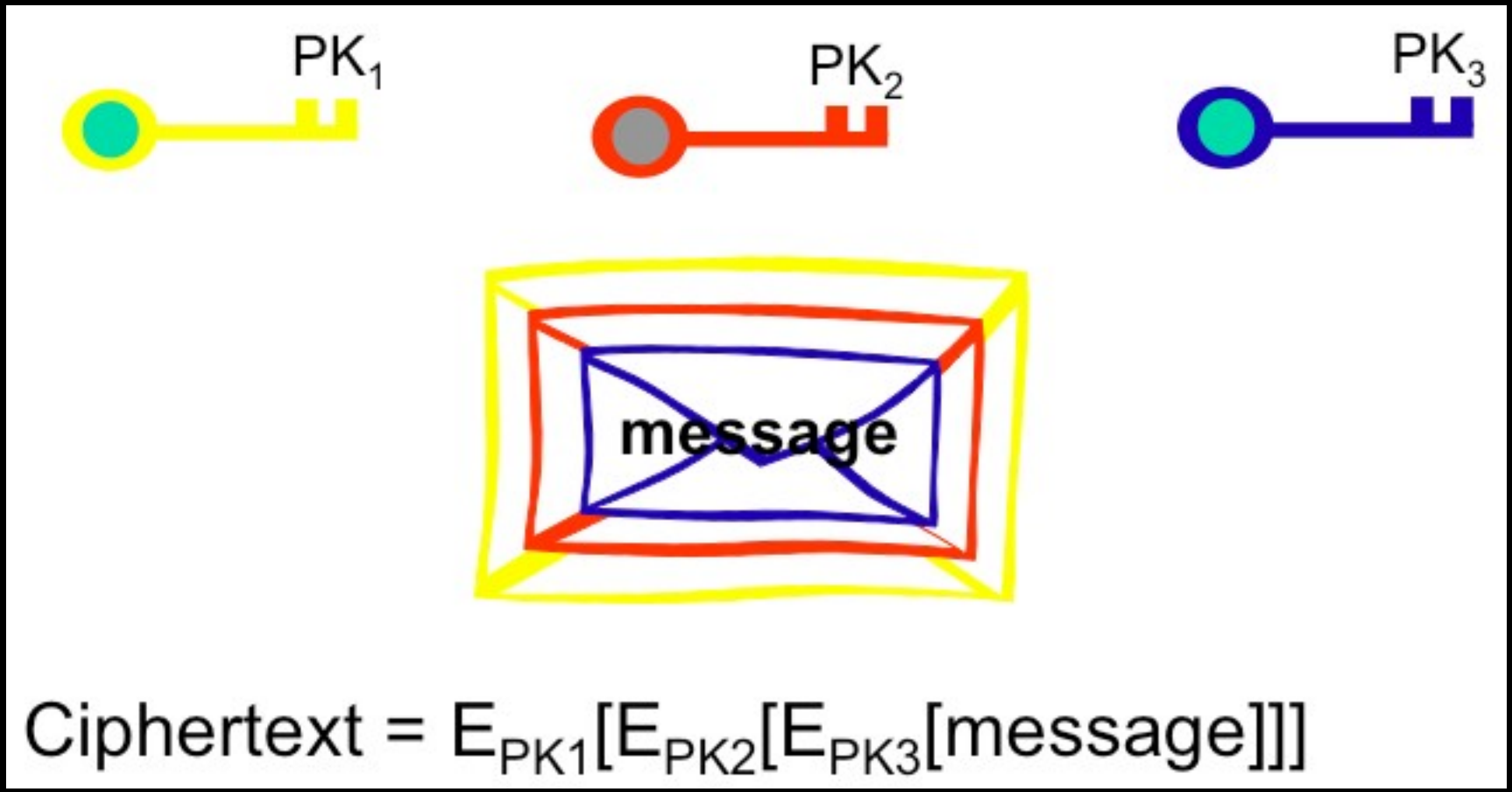
Mixes

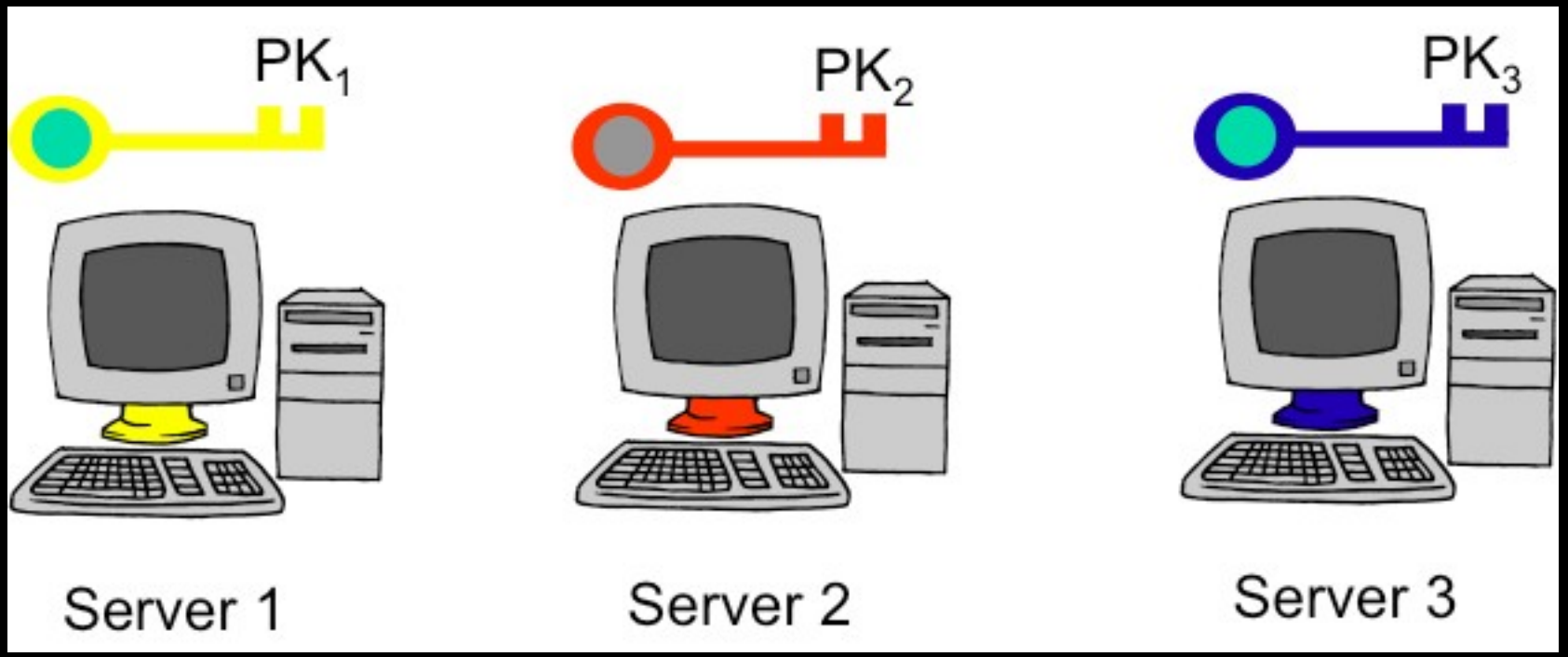


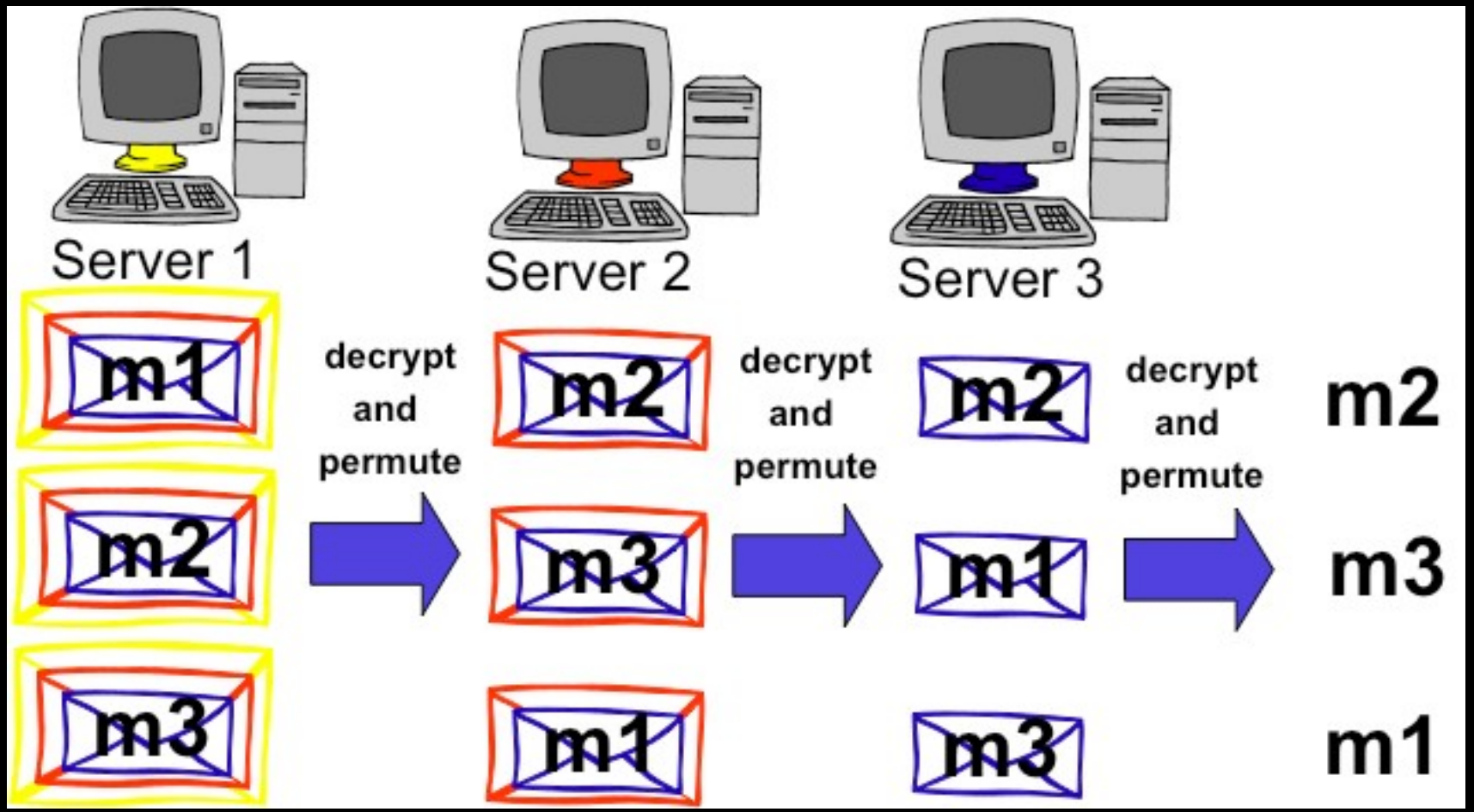


Randomly permutes and decrypts inputs


PK1
PK2
PK3
Server 1
Server 2
Server 3


PK1
PK2
PK3
message
Ciphertext = EPK1[EPK2[EPK3[message]]]


PK1
PK2
PK3
Server 1
Server 2
Server 3


Server 1
Server 2
Server 3
m1
m2
m3
decrypt and permute
m2
m3
m1
decrypt and permute
m2
m1
m3
decrypt and permute
m2
m3
m1

Mixes

- Invented by Chaum 1981 (not counting ancient Athens)
- As long as one mix is honest, network hides anonymity up to capacity of the mix
- Sort of
  - Flooding
  - Trickling
- Many variants
  - Timed
  - Pool
  - ...

Anonymous communications

Technical

Governmental/Social

1. What is it?

2. Why does it matter?

3. How do we build it?

1.
What is anonymity anyway?

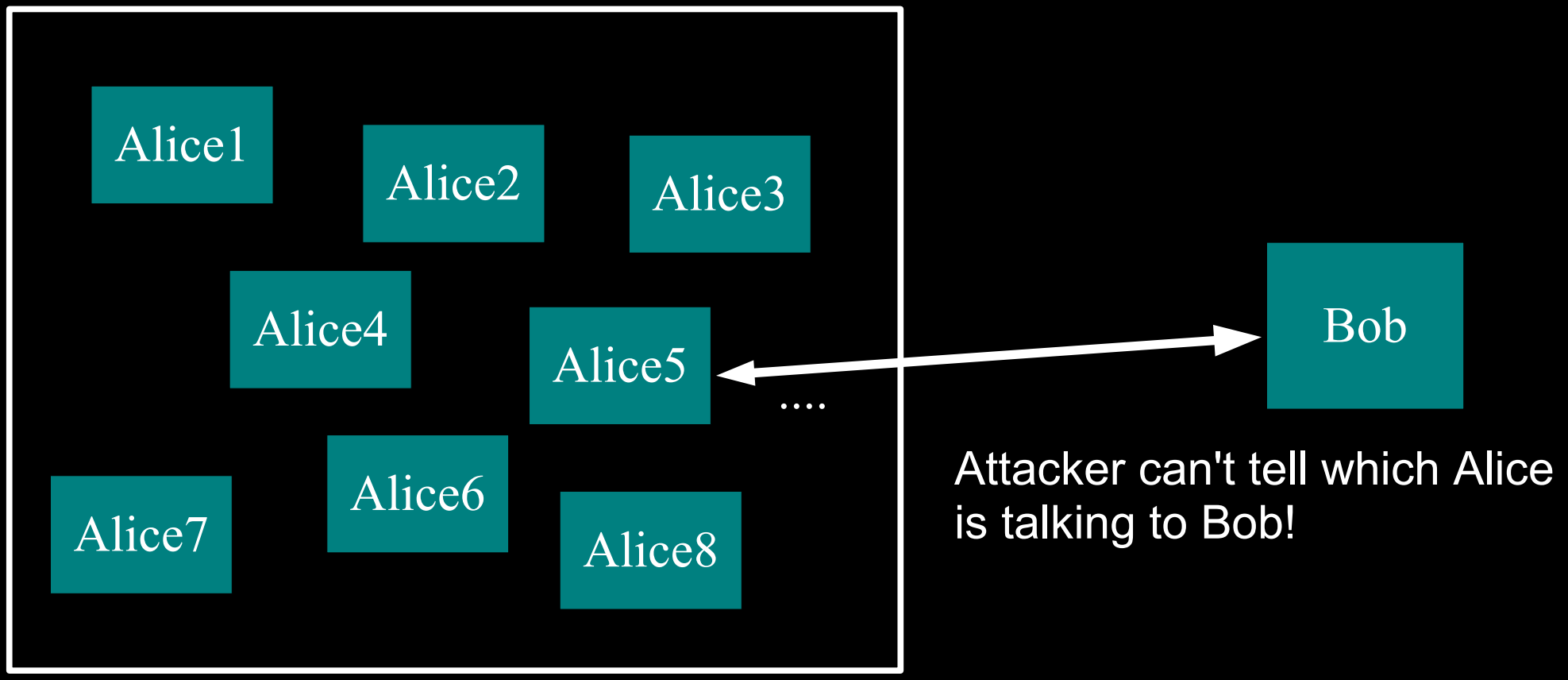
Informally: anonymity means you can't tell who did what

“Who wrote this blog post?”

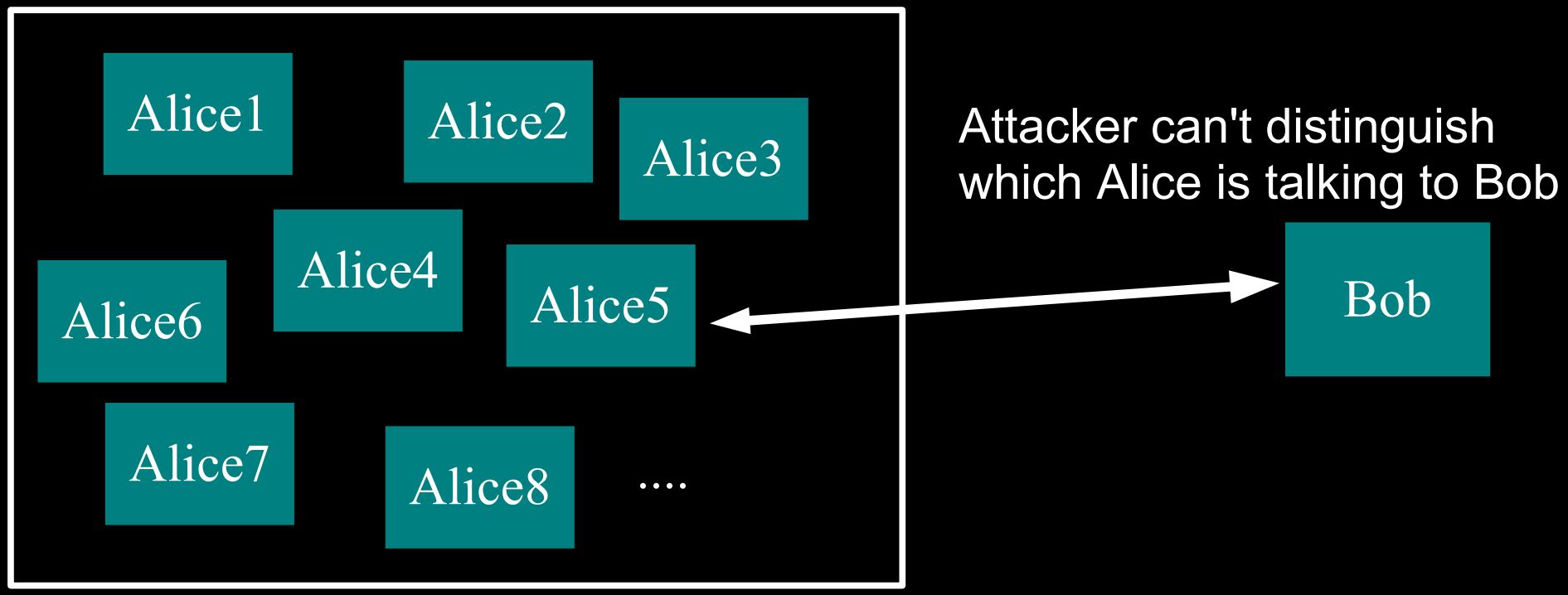
“Who's been viewing my webpages?”

“Who's been emailing patent attorneys?”

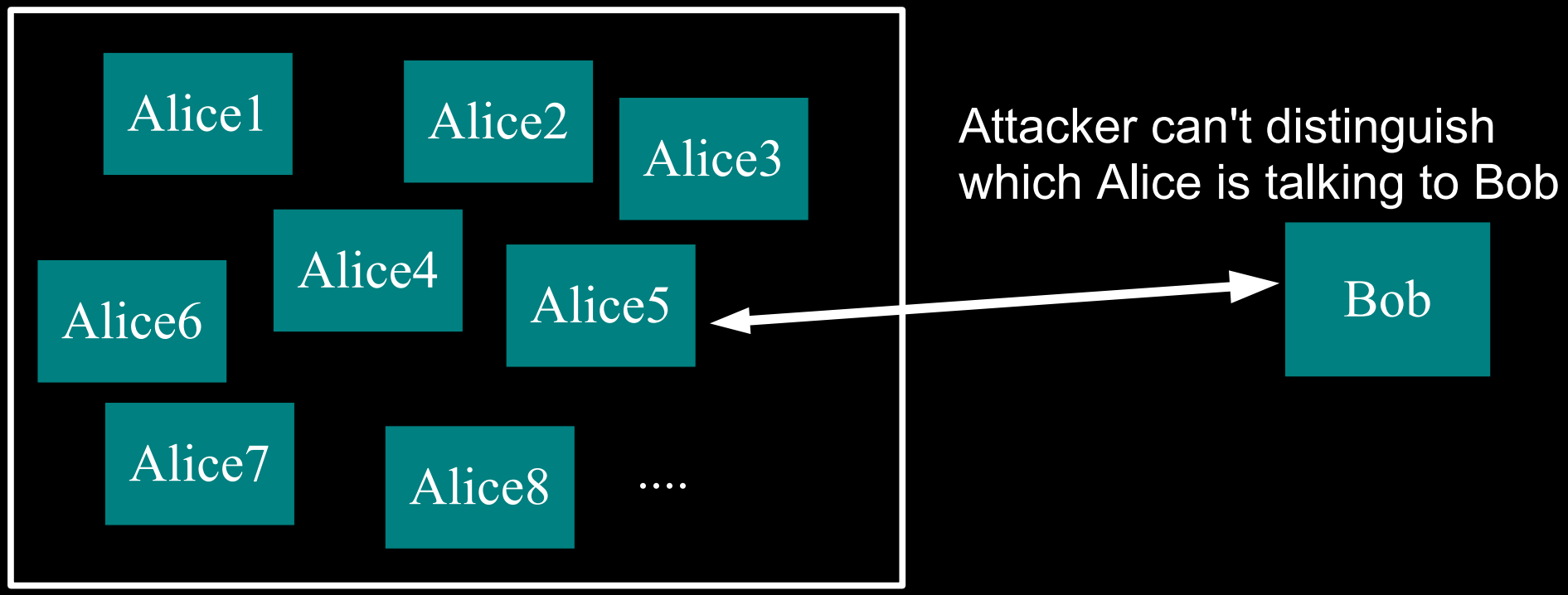
Formally: anonymity means indistinguishability within an "anonymity set"



Formally: anonymity means indistinguishability within an “anonymity set”

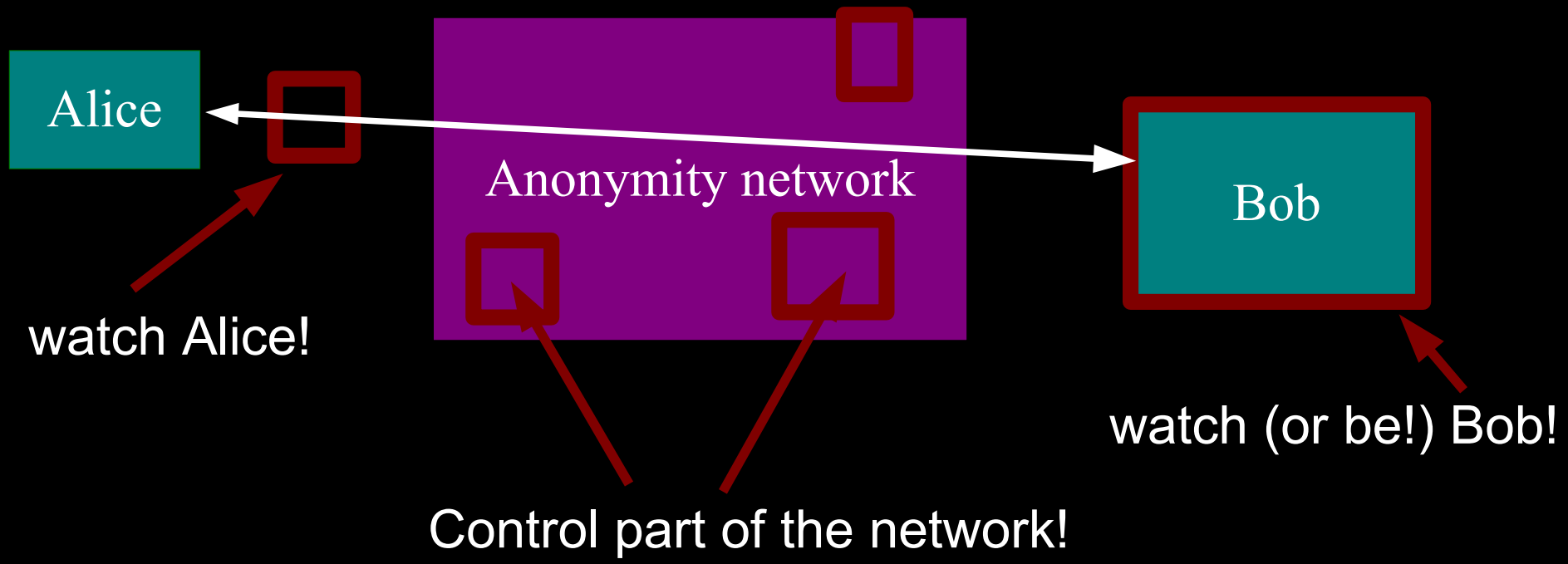


Formally: anonymity means indistinguishability within an “anonymity set”



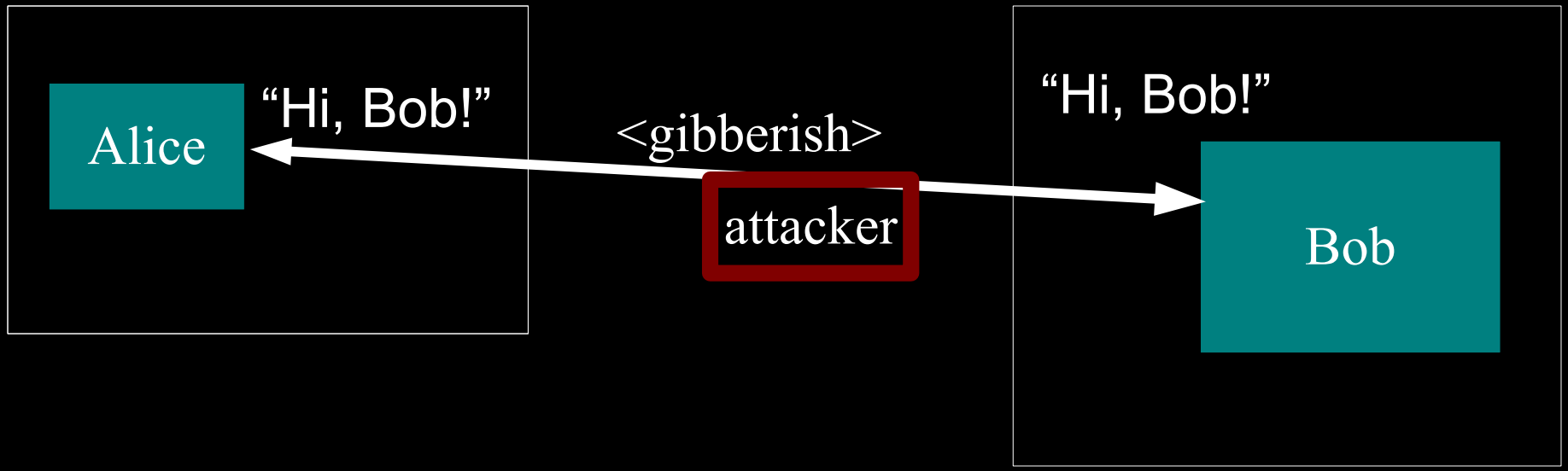
- Can't distinguish?
  - Basic anonymity set size
  - Probability distribution within anonymity set
  - ....

We have to make some assumptions about what the attacker can do.

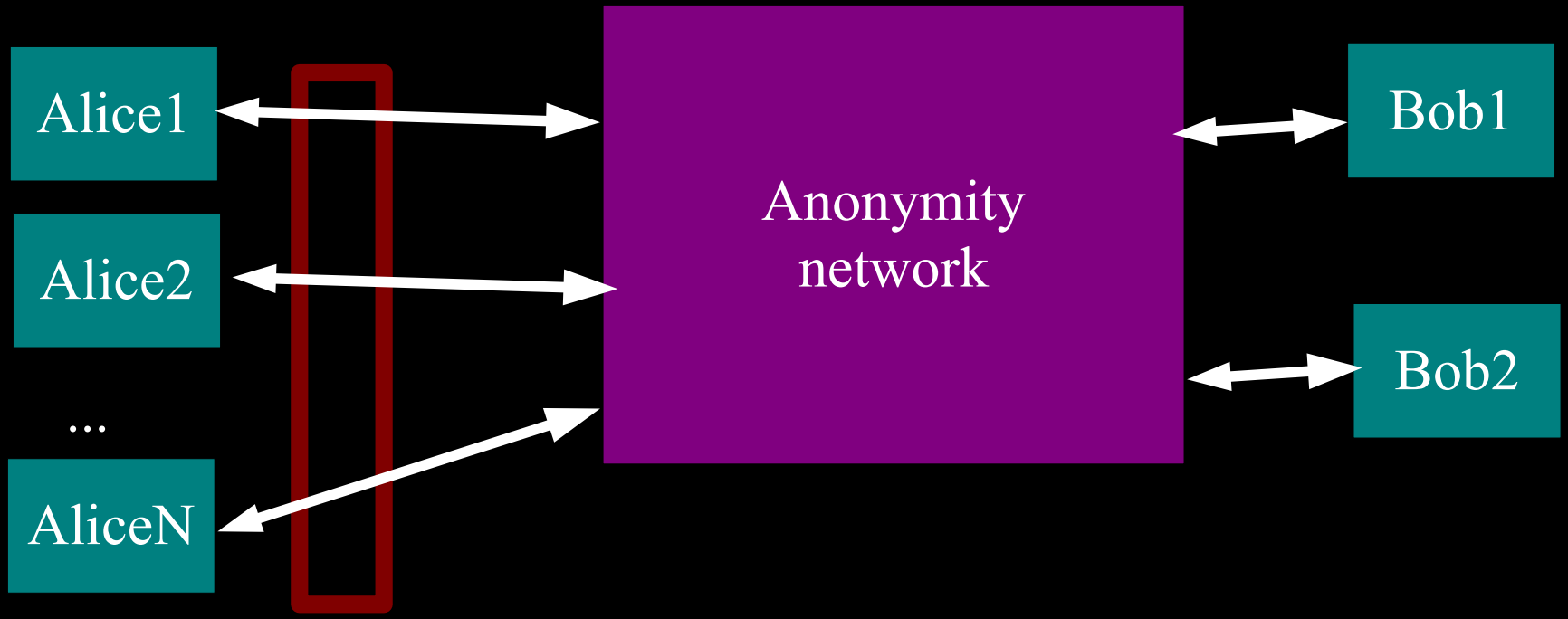


Etc, etc.

Anonymity isn't confidentiality: Encryption just protects contents.



Anonymity isn't steganography: Attacker can tell that Alice is talking; just not to whom.



Anonymity isn't just wishful thinking...

“You can't prove it was me!”

“Promise you won't look!”

“Promise you won't remember!”

“Promise you won't tell!”

“I didn't write my name on it!”

“Isn't the Internet already anonymous?”

...since “weak” anonymity... isn't.

~~“You can't prove it was me!”~~

*Proof is a **very** strong word.*
With statistics,
suspicion becomes certainty.

Will others parties have the ability and incentives to keep their promises?

~~“Promise you won't look!”~~

~~“Promise you won't remember!”~~

~~“Promise you won't tell!”~~

~~“I didn't write my name on it!”~~

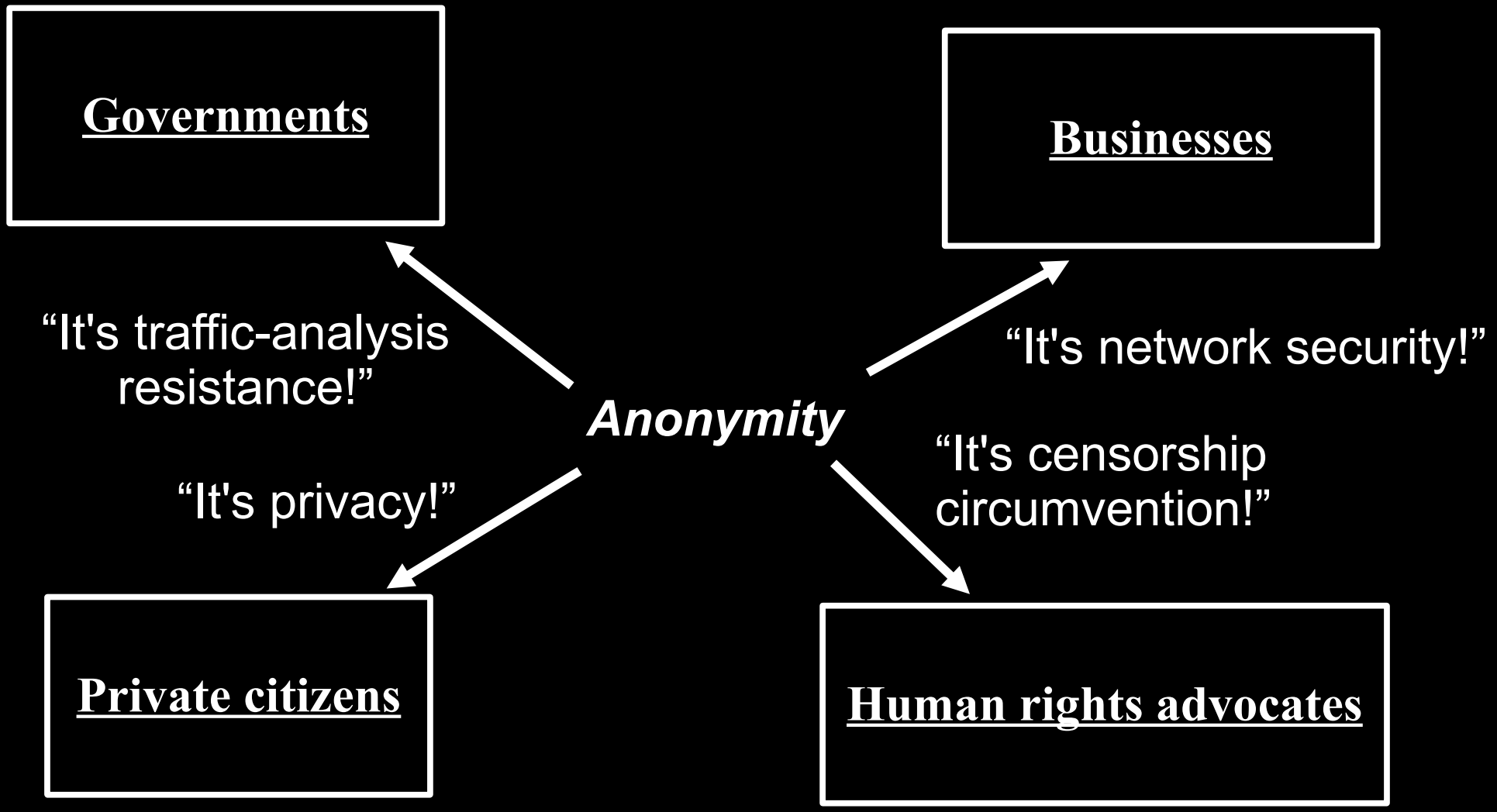
Not what we're talking about.

Nope!
(More info later.)

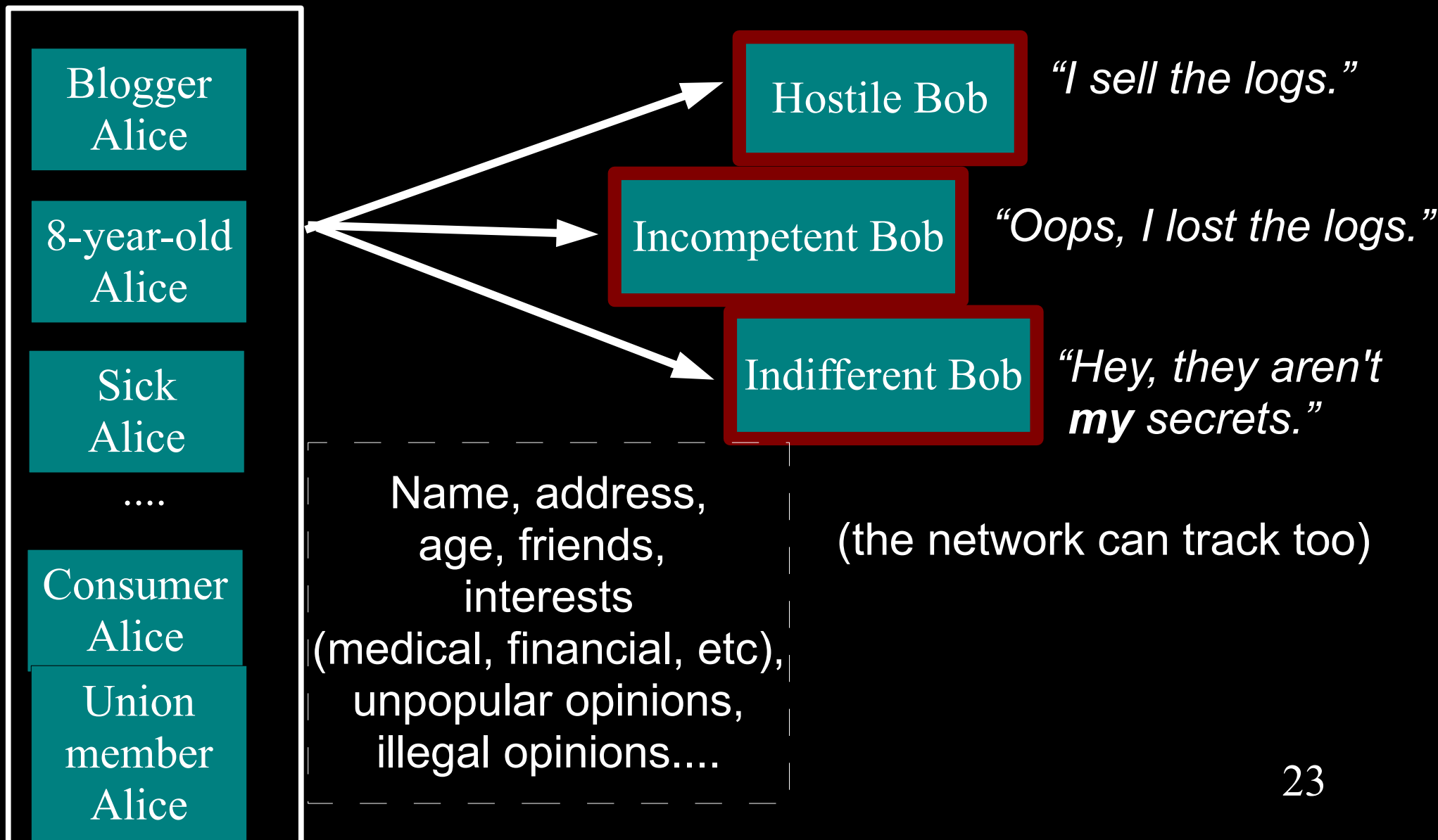
~~“Isn't the Internet already anonymous?”~~

2. **Why does anonymity matter?**

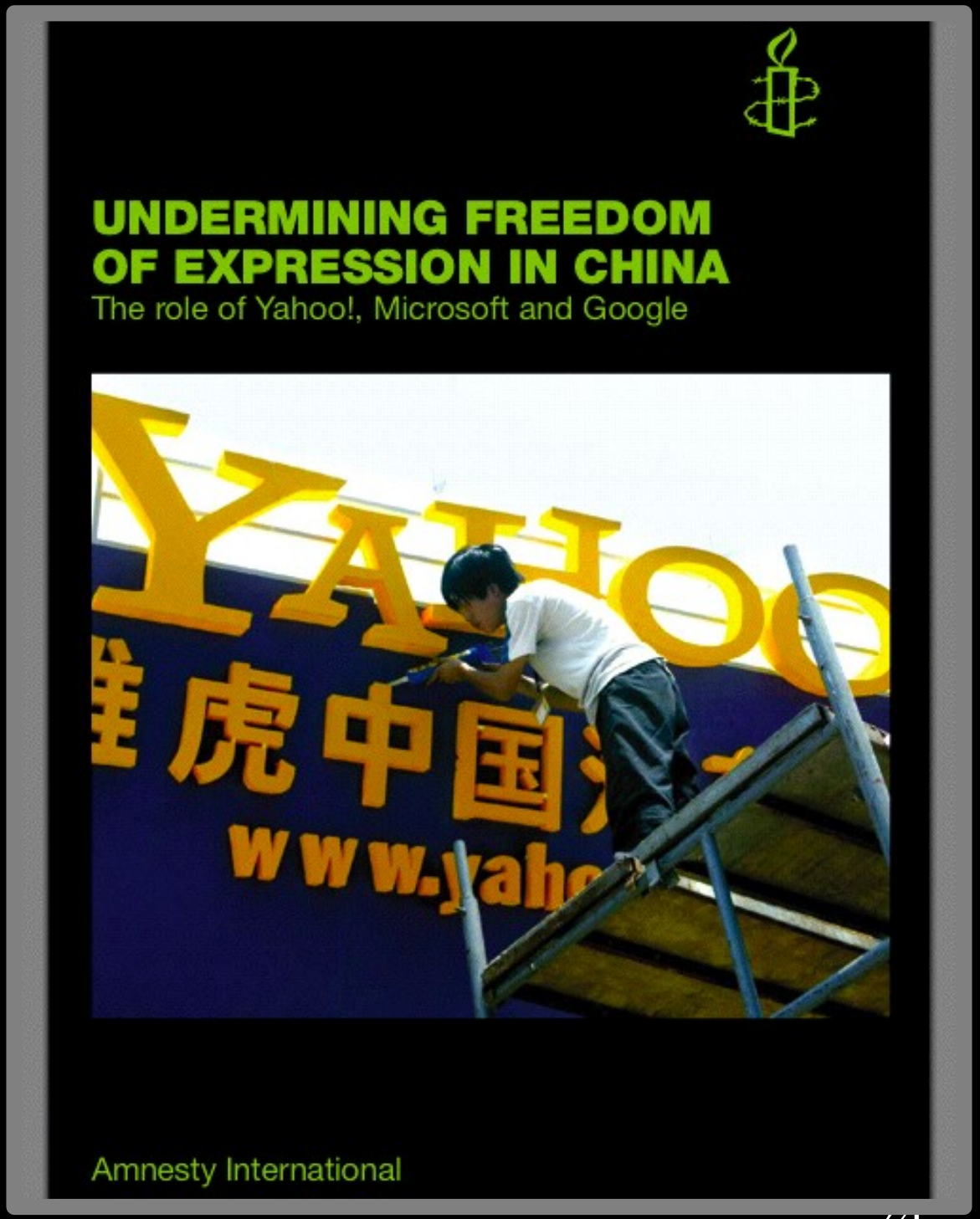
Anonymity serves different interests for different user groups.



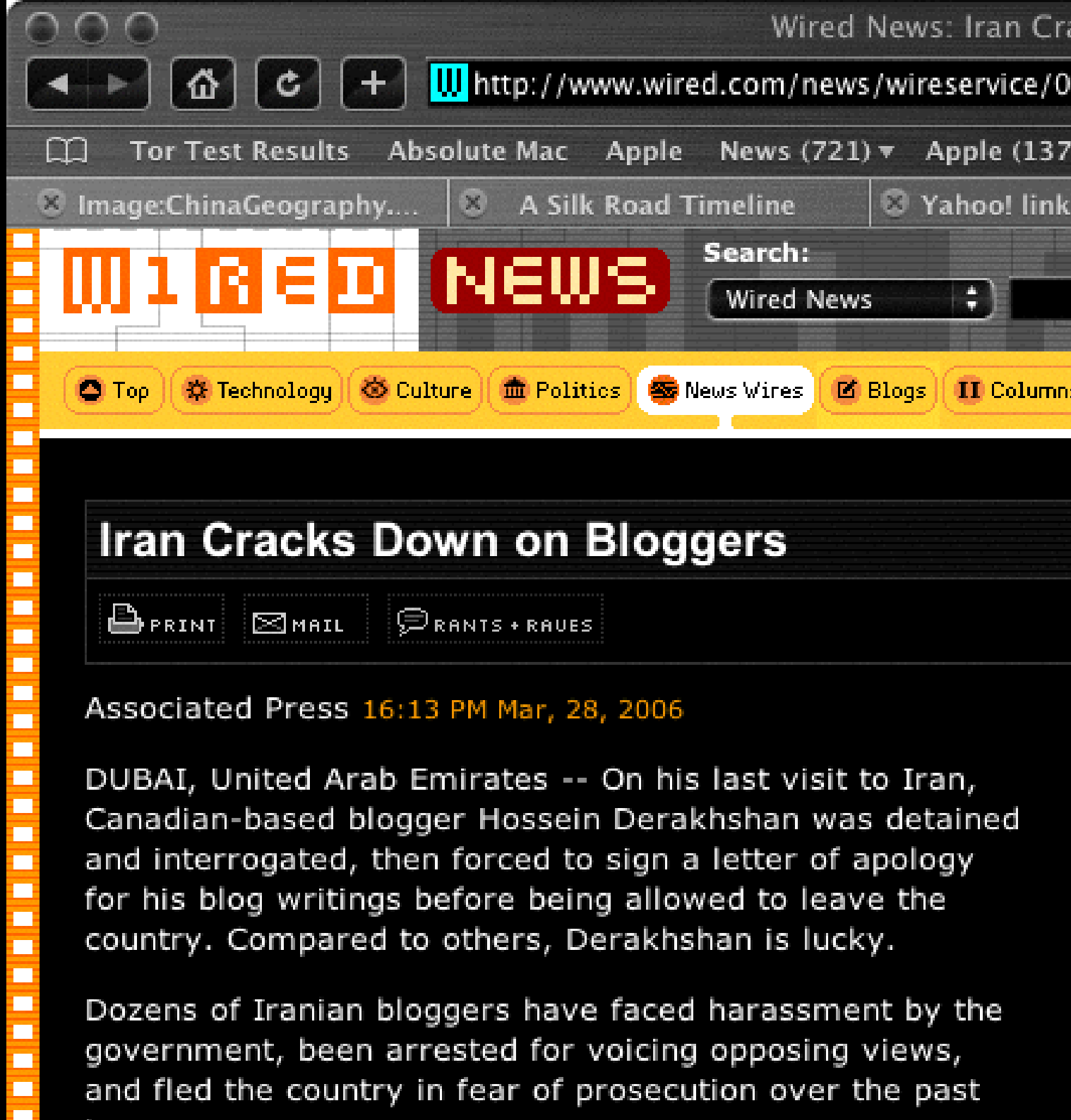
Regular citizens don't want to be watched and tracked.



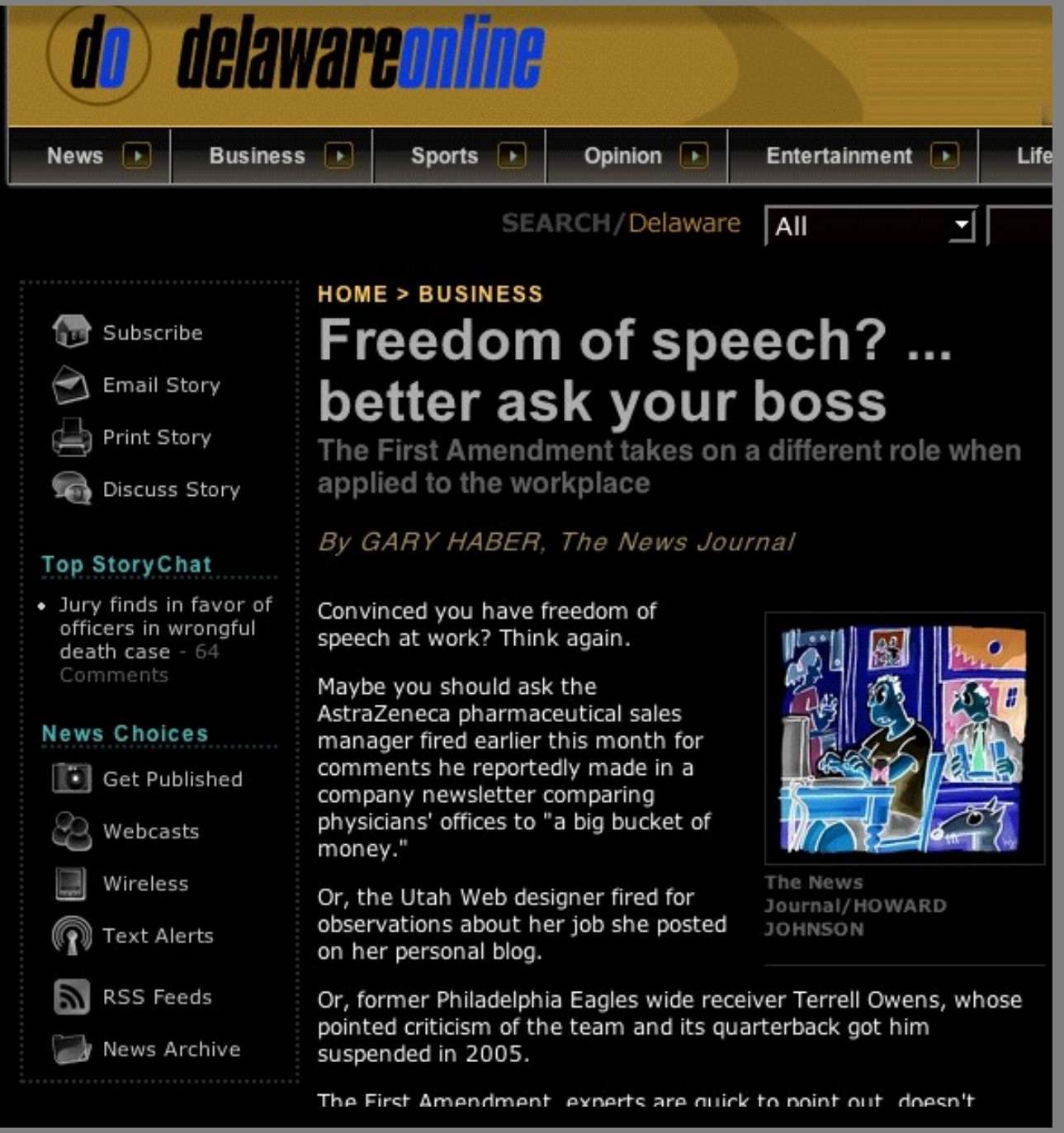
Many people don't get to see the internet that you can see...



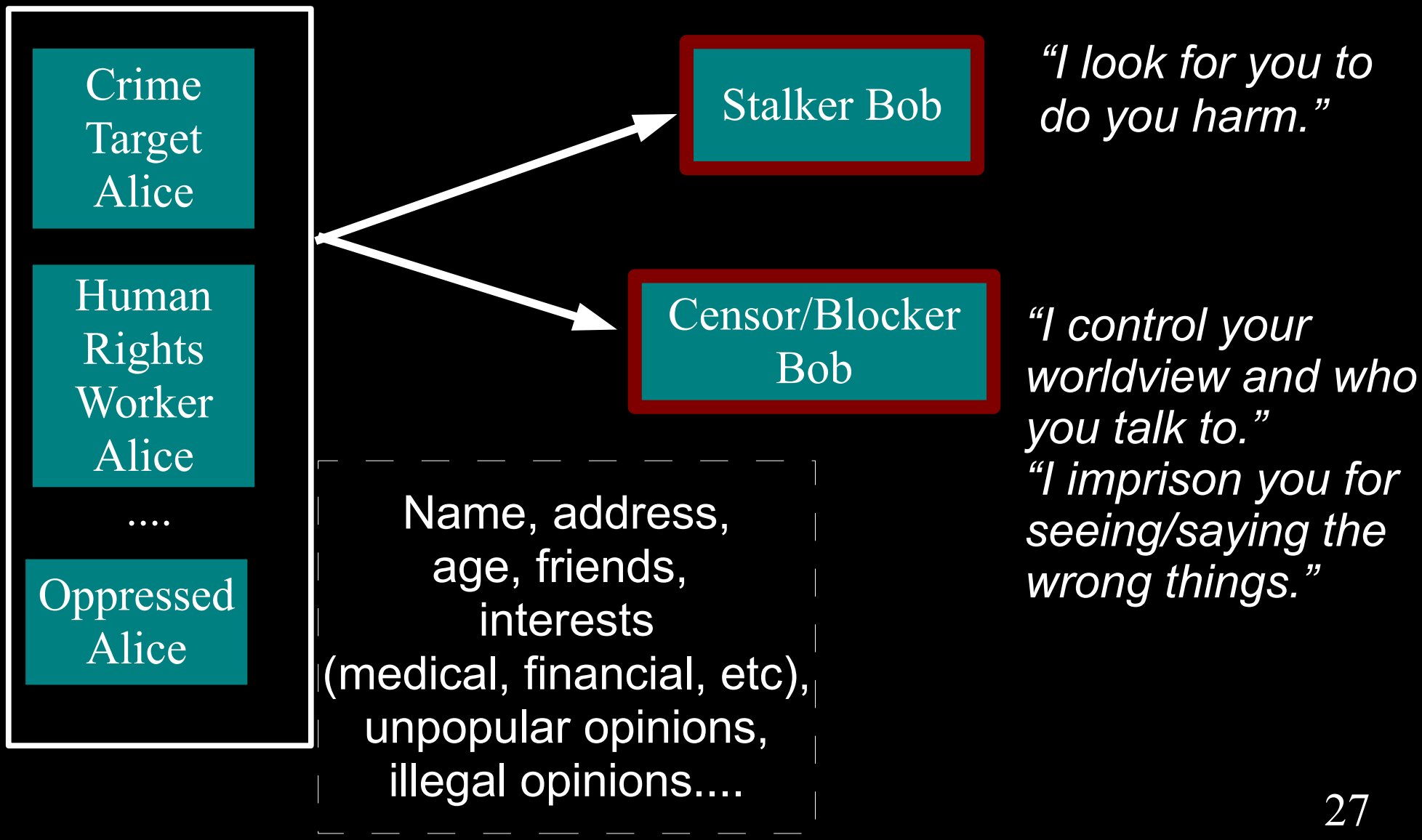
and they can't speak on the internet either...



It's not only about dissidents in faraway lands

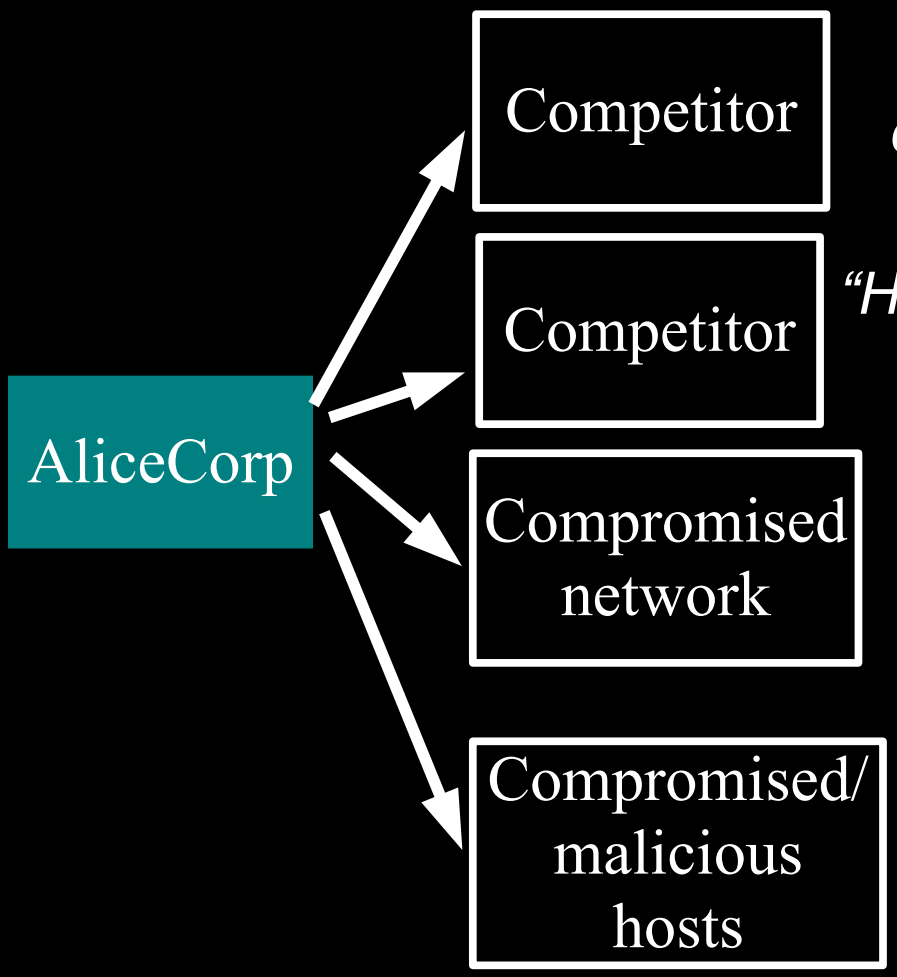


Regular citizens don't want to be watched and tracked.



Law enforcement needs anonymity to get the job done.

Businesses need to protect trade secrets... and their customers.



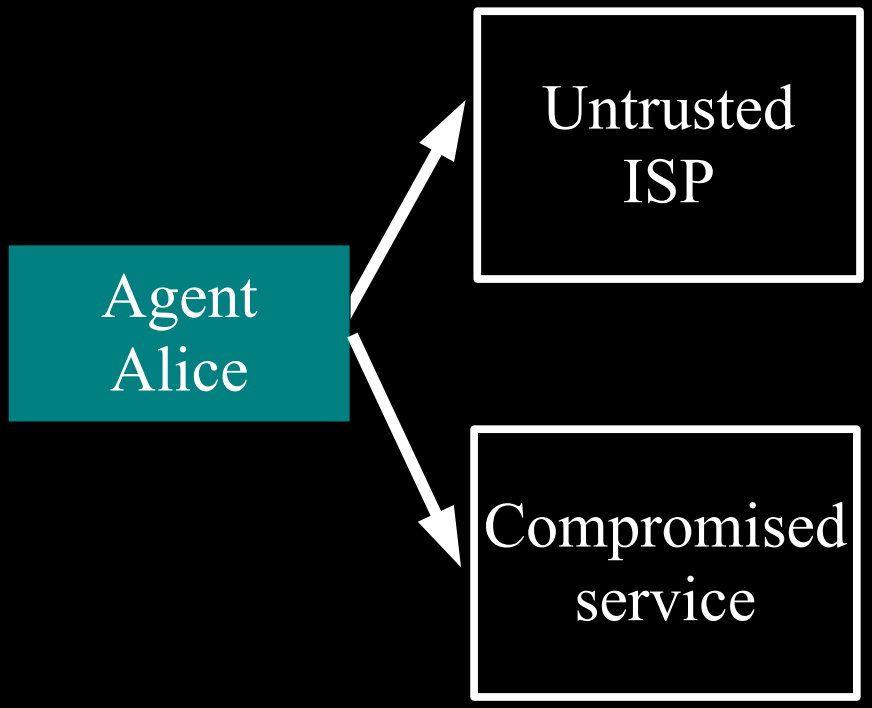
"Oh, your employees are reading our patents/jobs page/product sheets?"

"Hey, it's Alice! Give her the 'Alice' version!"

"Wanna buy a list of Alice's suppliers? What about her customers? What about her engineering department's favorite search terms?"

"We attack Alice's customers with malware, and watch for when she notices us."

Governments need anonymity for their security

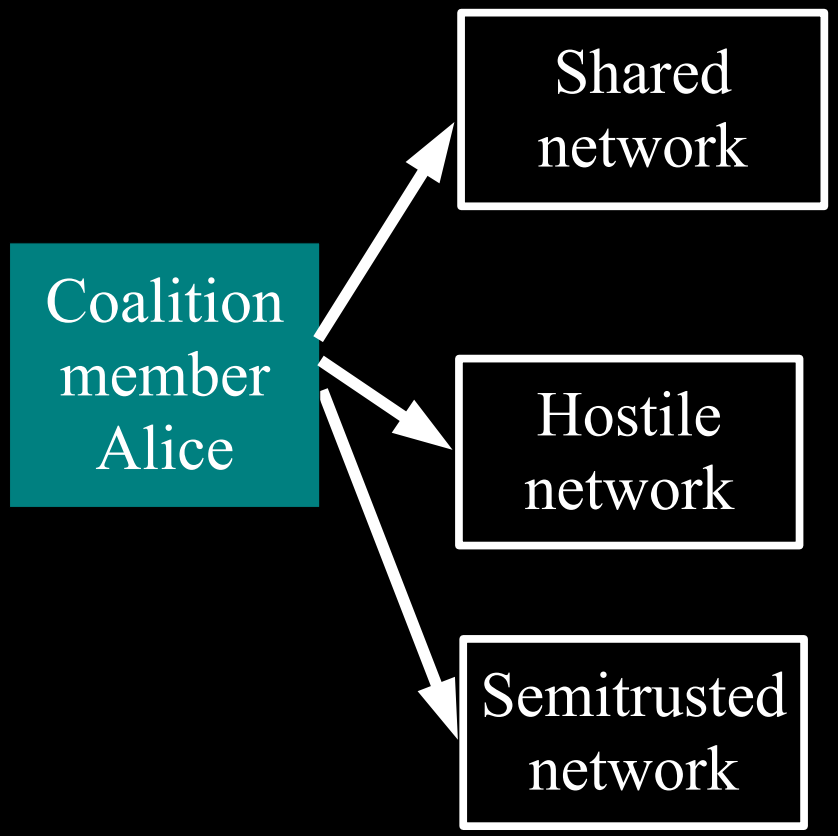


"What will you bid for a list of Baghdad IP addresses that get email from .gov?"

"What bid for the hotel room from which someone just logged in to foo.navy.mil?"

"What *does* the CIA Google for?"

Governments need anonymity for their security



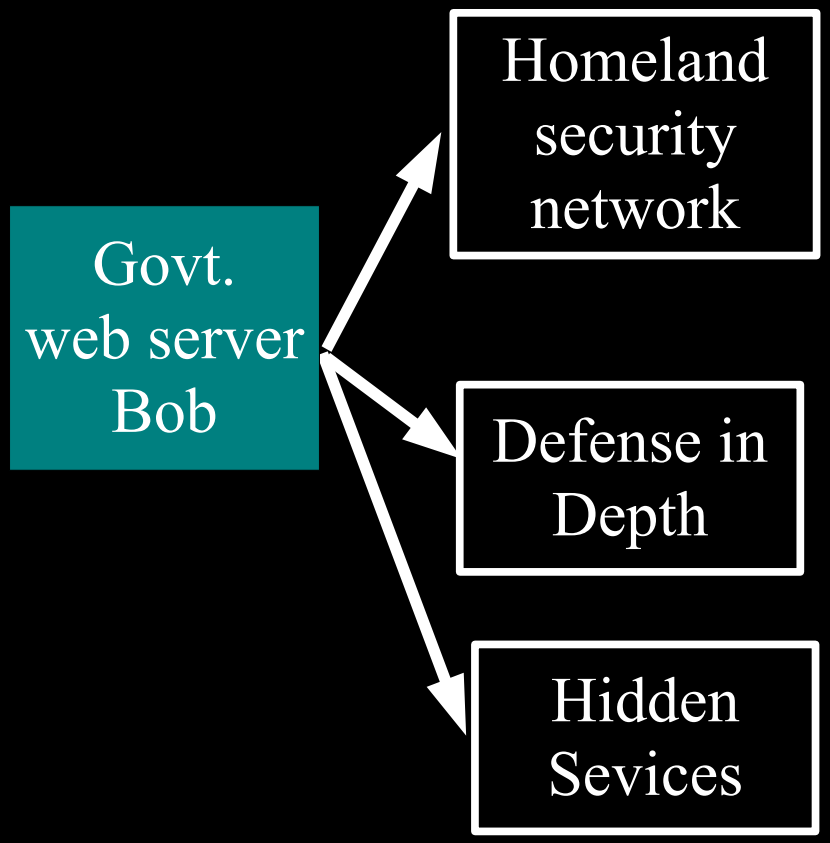
"Do I really want to reveal my internal network topology?"

"Do I want all my partners to know extent/pattern of my comms with other partners?"

"How can I establish communication with locals without a trusted network?"

"How can I avoid selective blocking of my communications?"

Governments need anonymity for their security



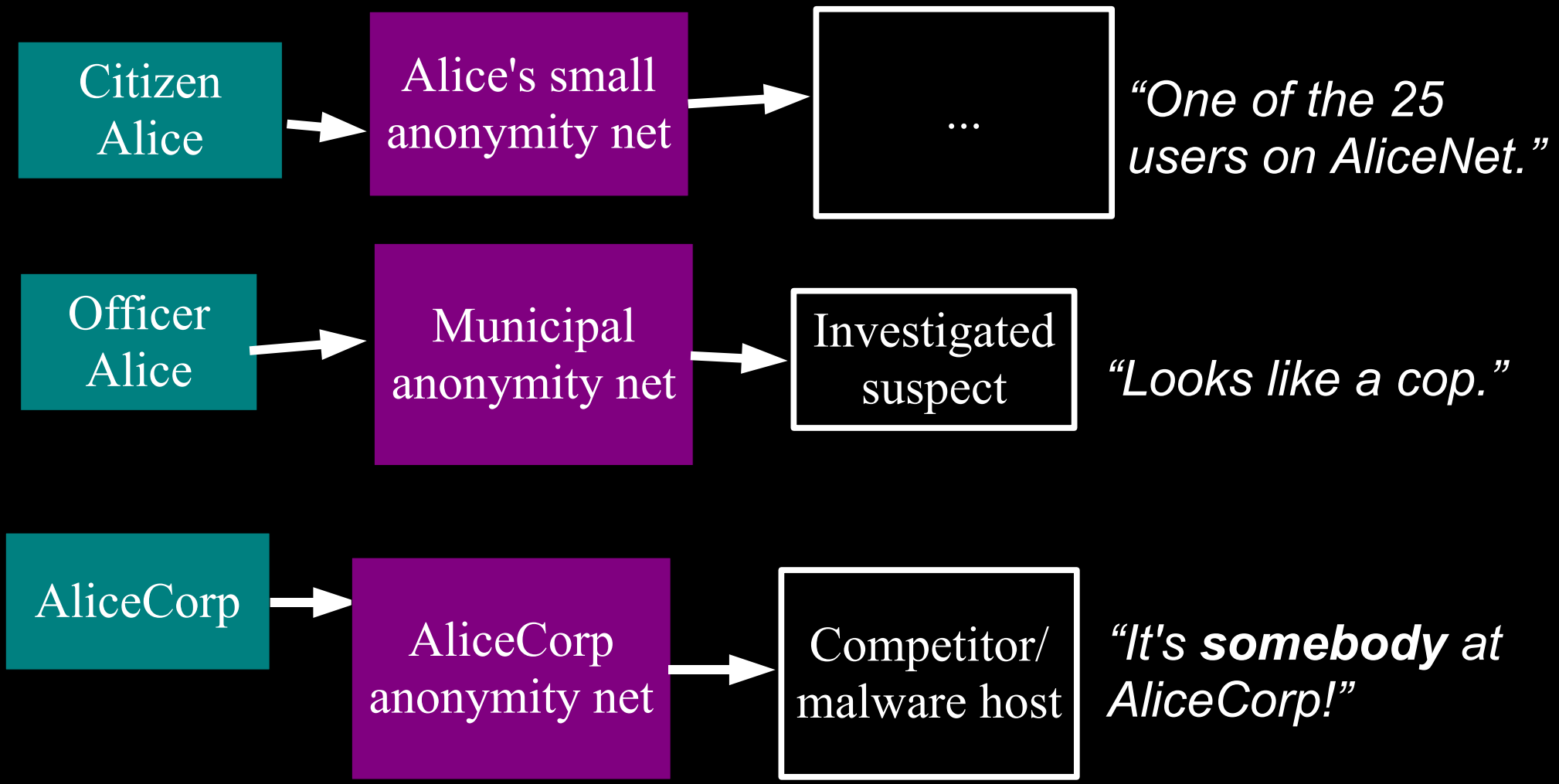
"How can I securely and quickly exchange vital info with every sheriff's dept and Hazmat transporter without bringing them into my secure network?

"Do I want every SIPRNET node to know where all the traffic on it is headed?"

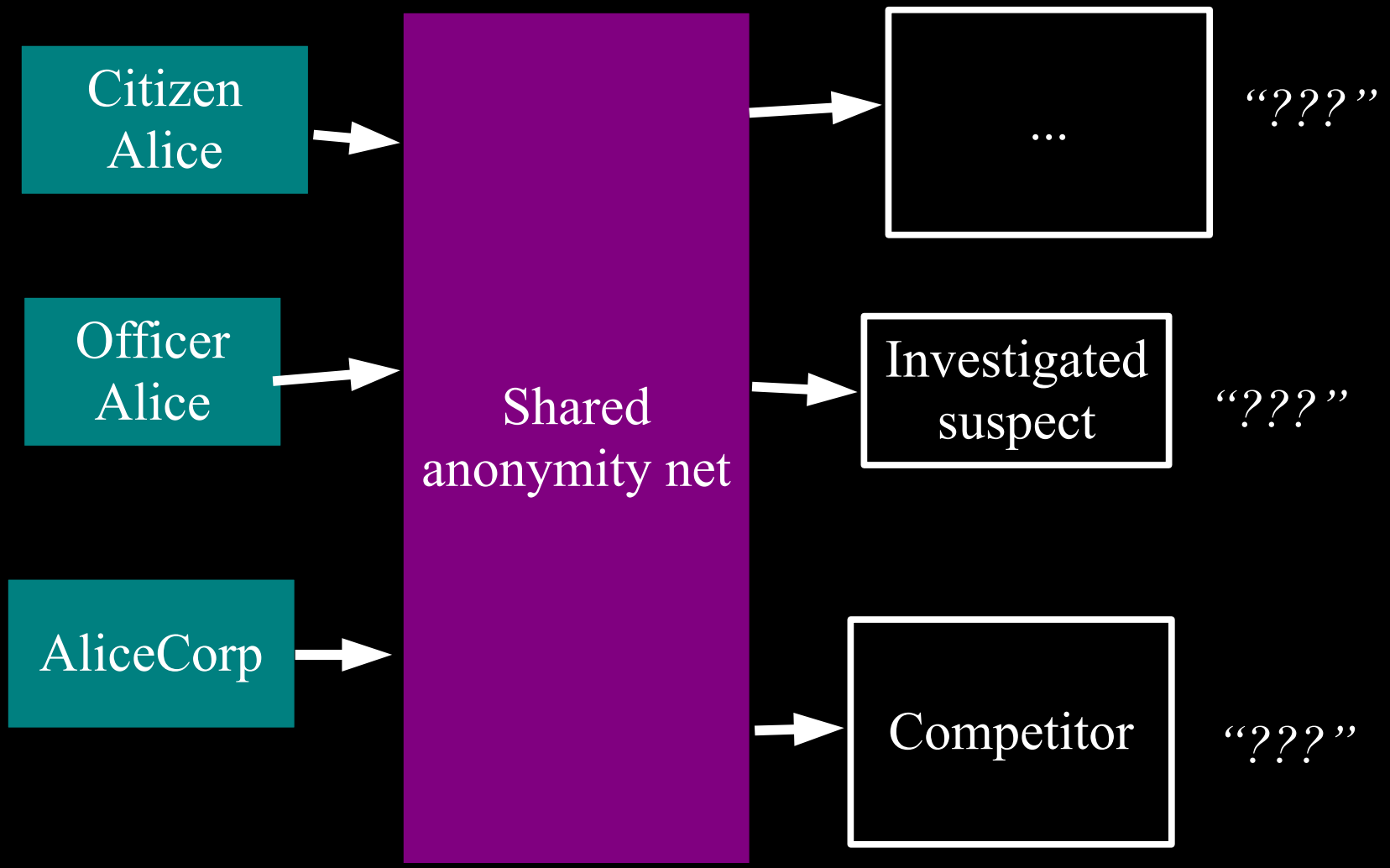
"Can I hide where my MLS chat server/my automated regrader is?"

Can my servers resist DDoS and physical attack even by authorized users?"

You can't be anonymous by yourself: private solutions are ineffective…

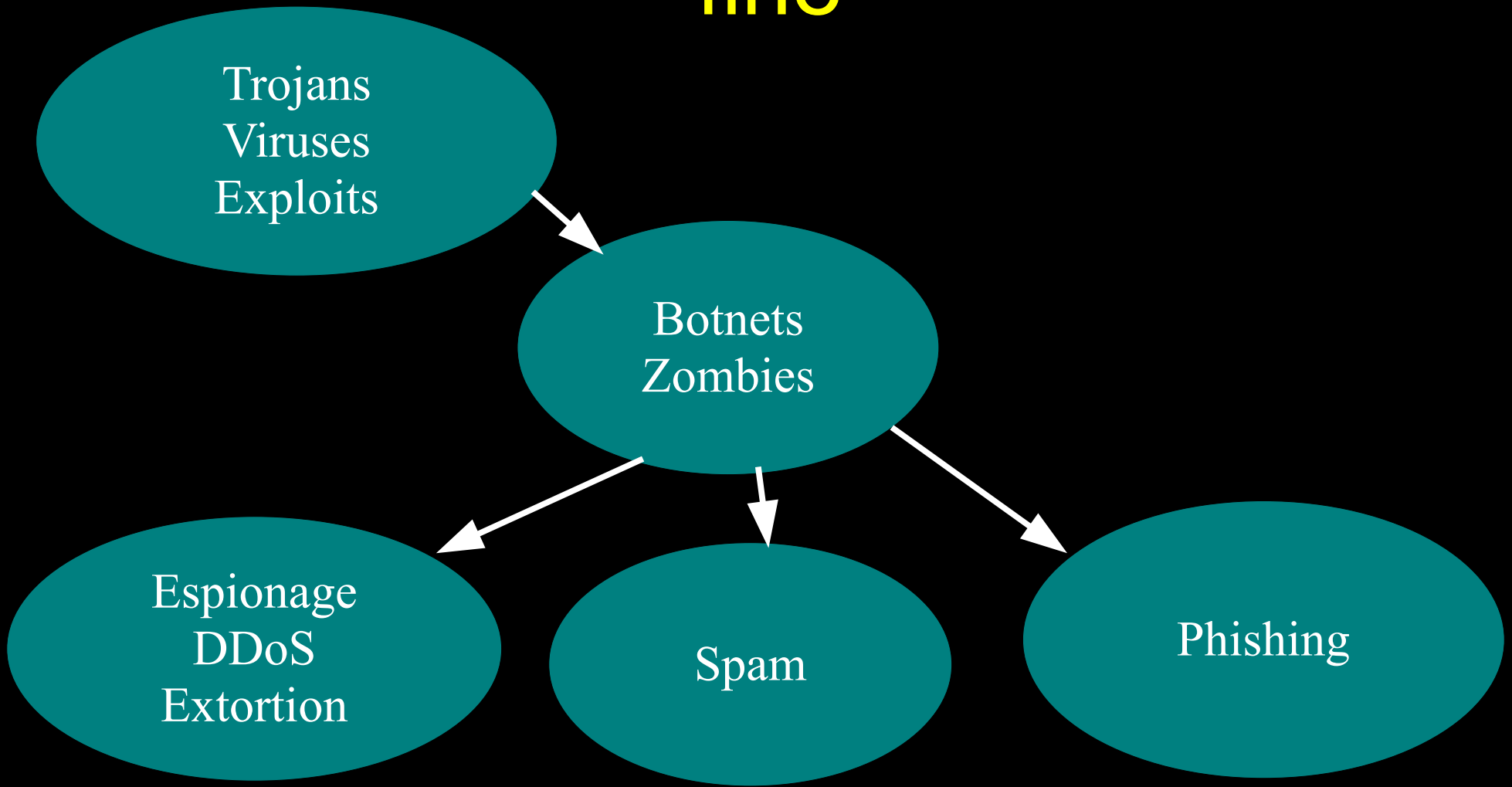


... so, anonymity loves company!

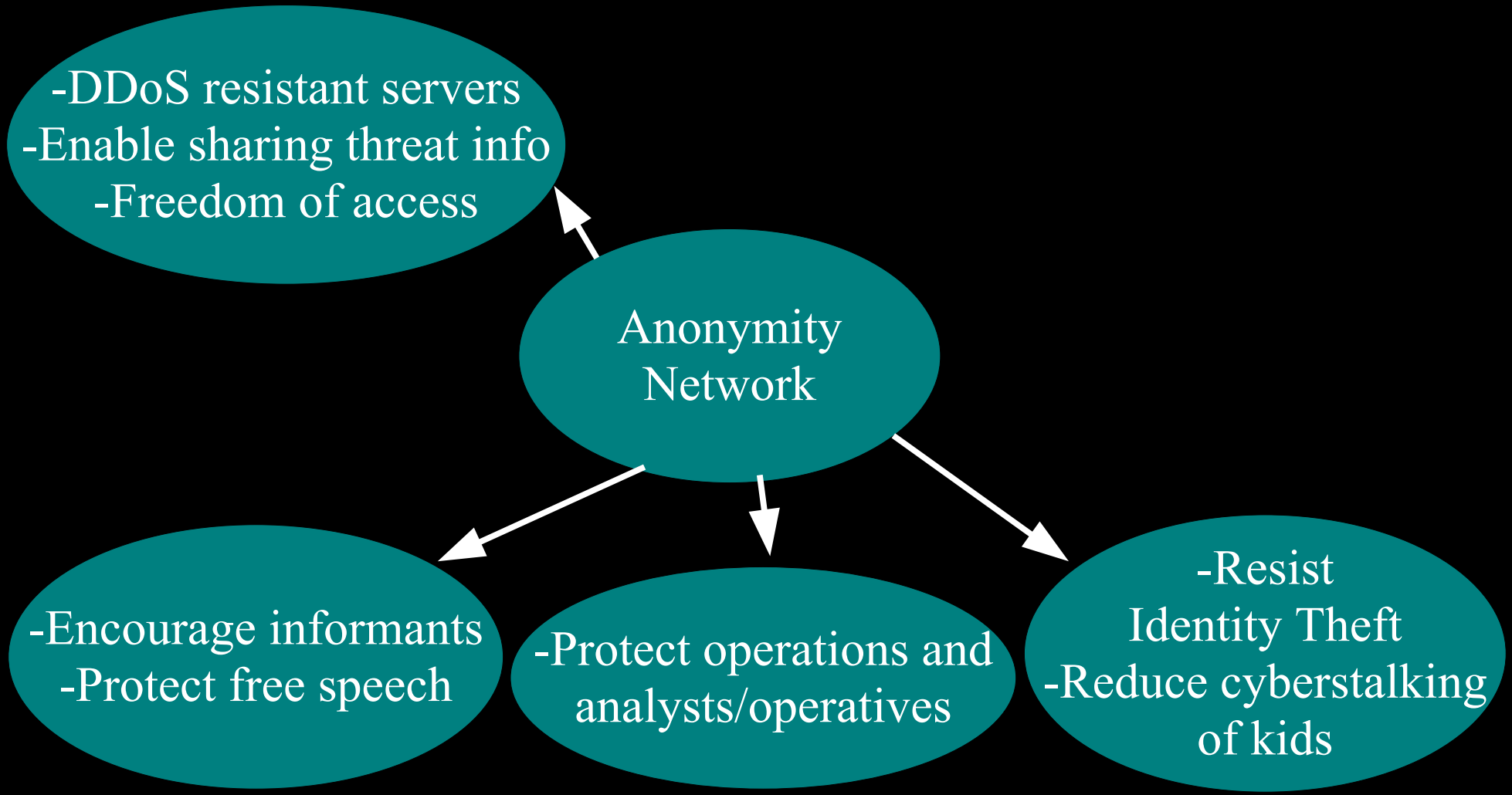


Don't bad people use anonymity?

Current situation: Bad people on internet are doing fine

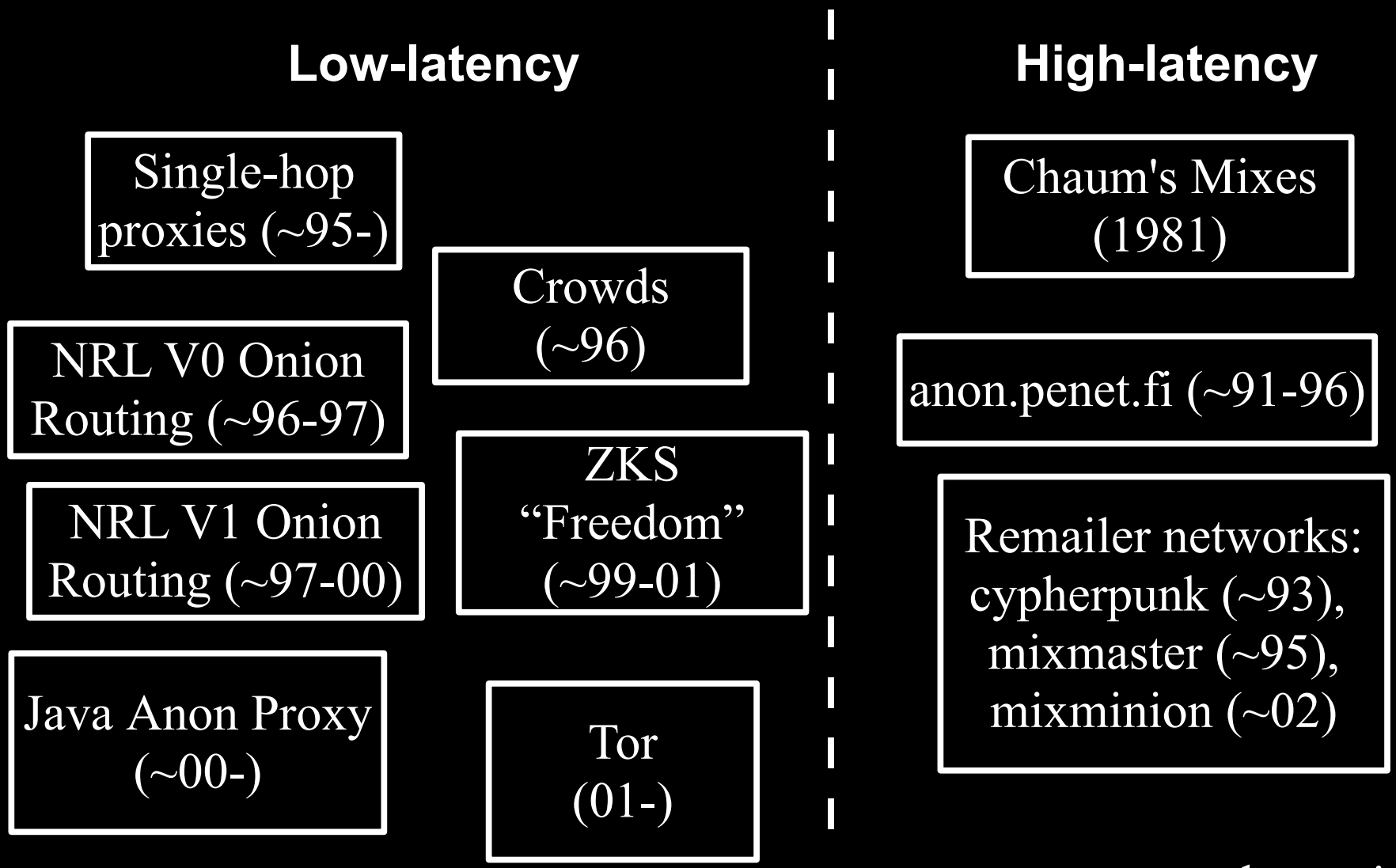


Giving good people a fighting chance

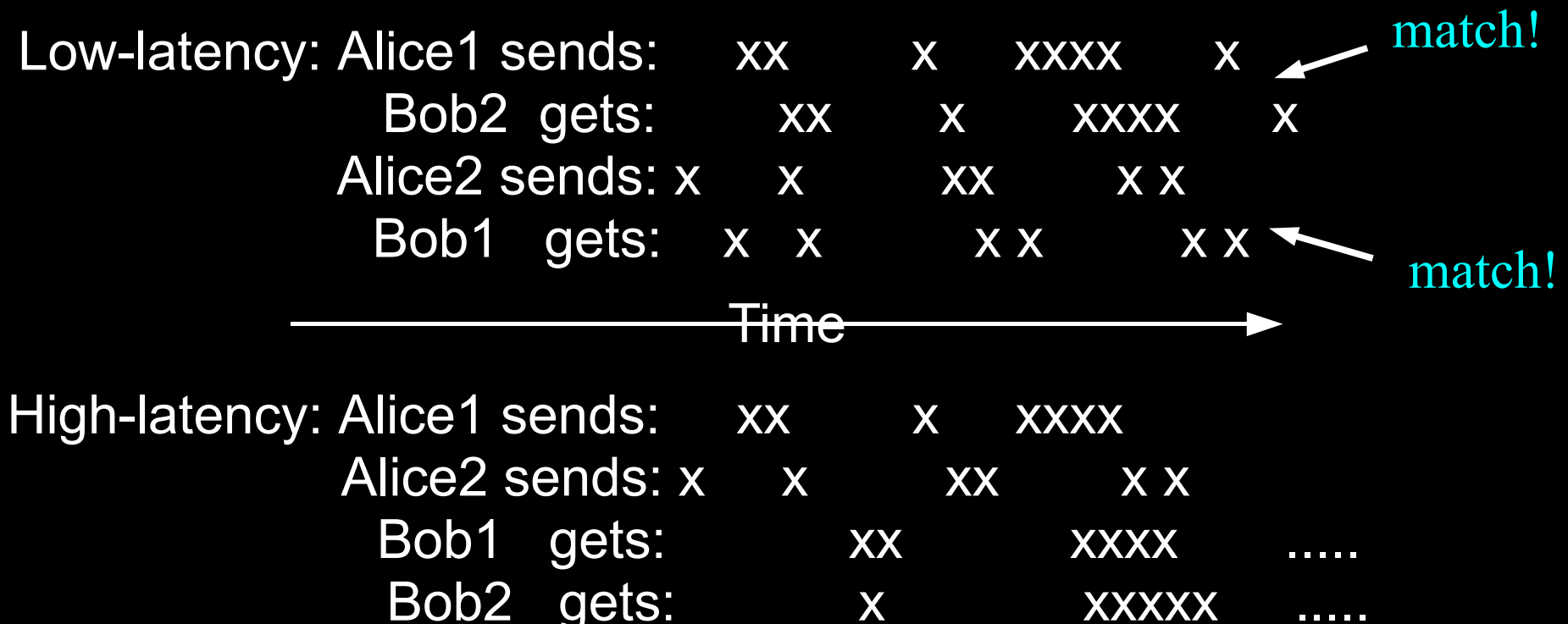


3. How does anonymity work?

Anonymity Systems for the Internet



Low-latency systems are vulnerable to end-to-end correlation attacks.



These attacks work in practice. The obvious defenses are expensive (like high-latency), useless, or both.

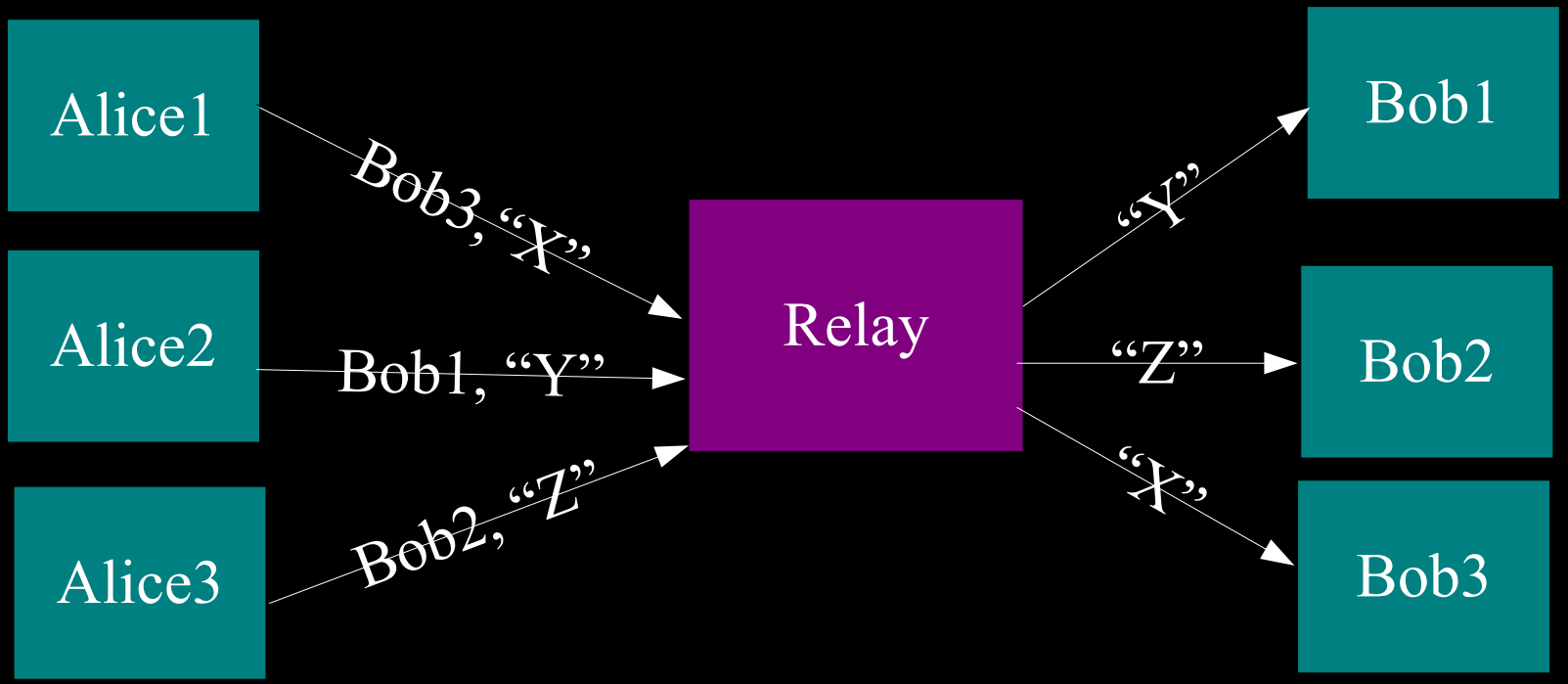
Still, we focus on low-latency, because it's more useful.

Interactive apps: web, IM, VOIP, ssh, X11, ...
 # users: millions?

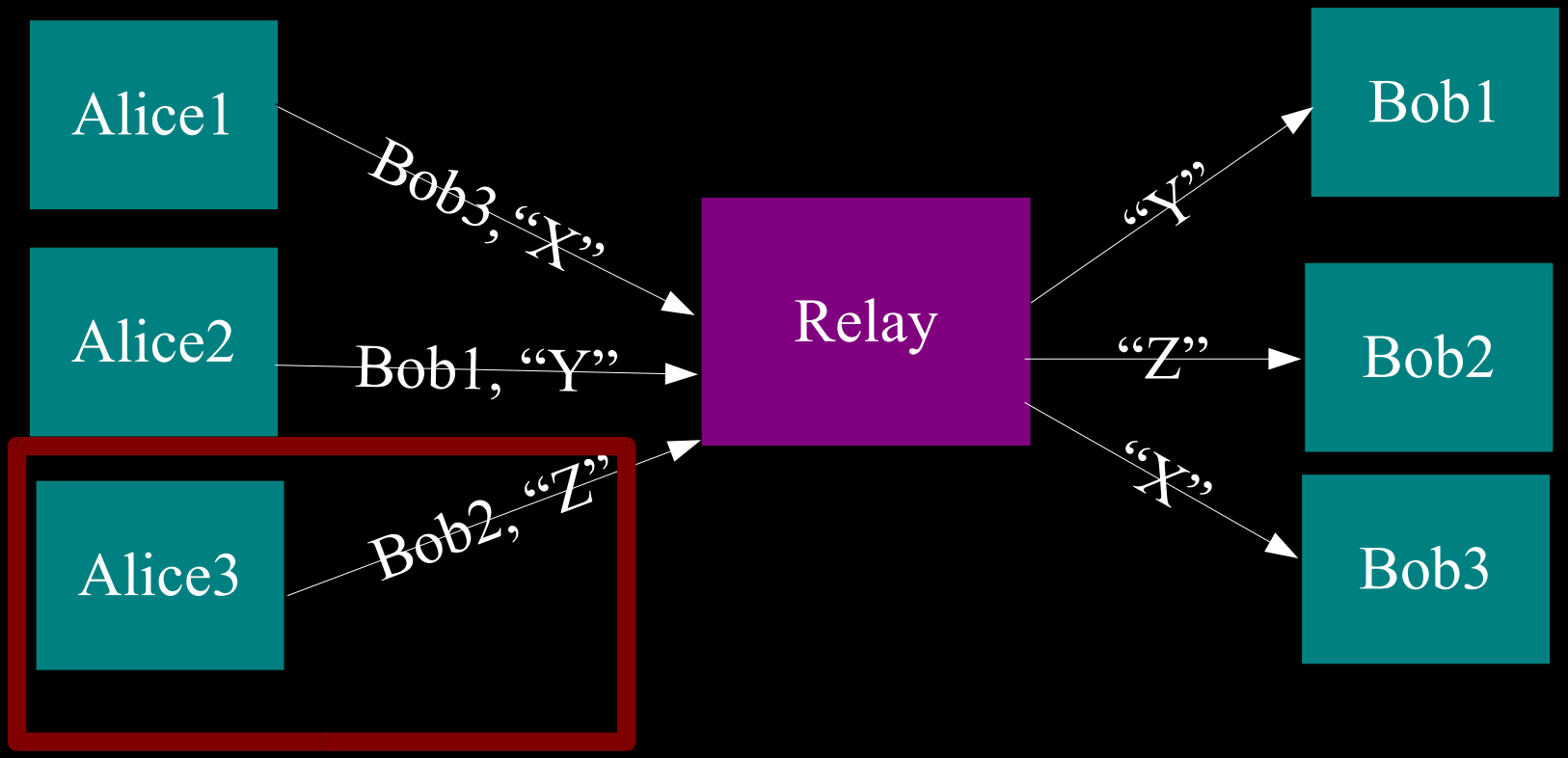
Apps that accept multi-hour delays and high bandwidth overhead: email, sometimes.
 # users: hundreds at most?

And if anonymity loves company....?

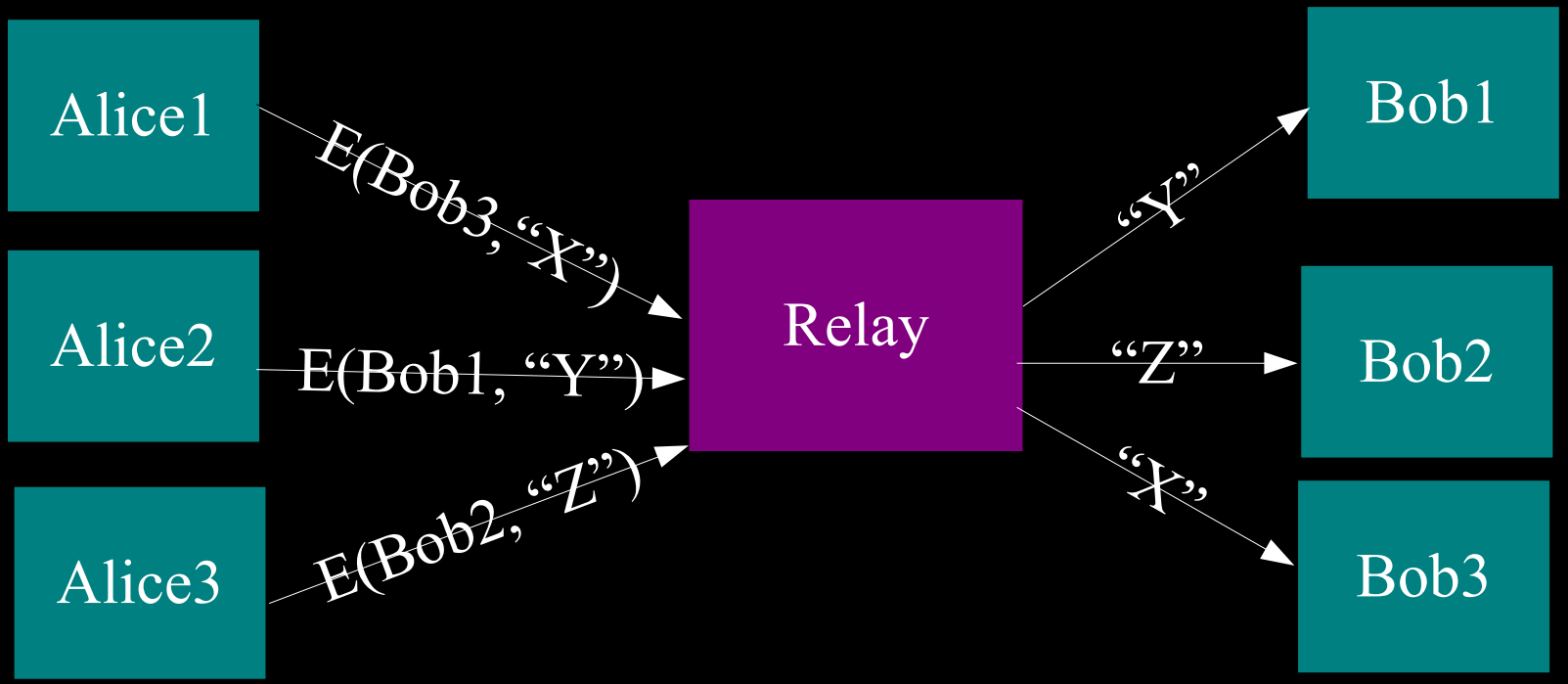
The simplest designs use a single relay to hide connections.



But an attacker who sees Alice can see who she's talking to.

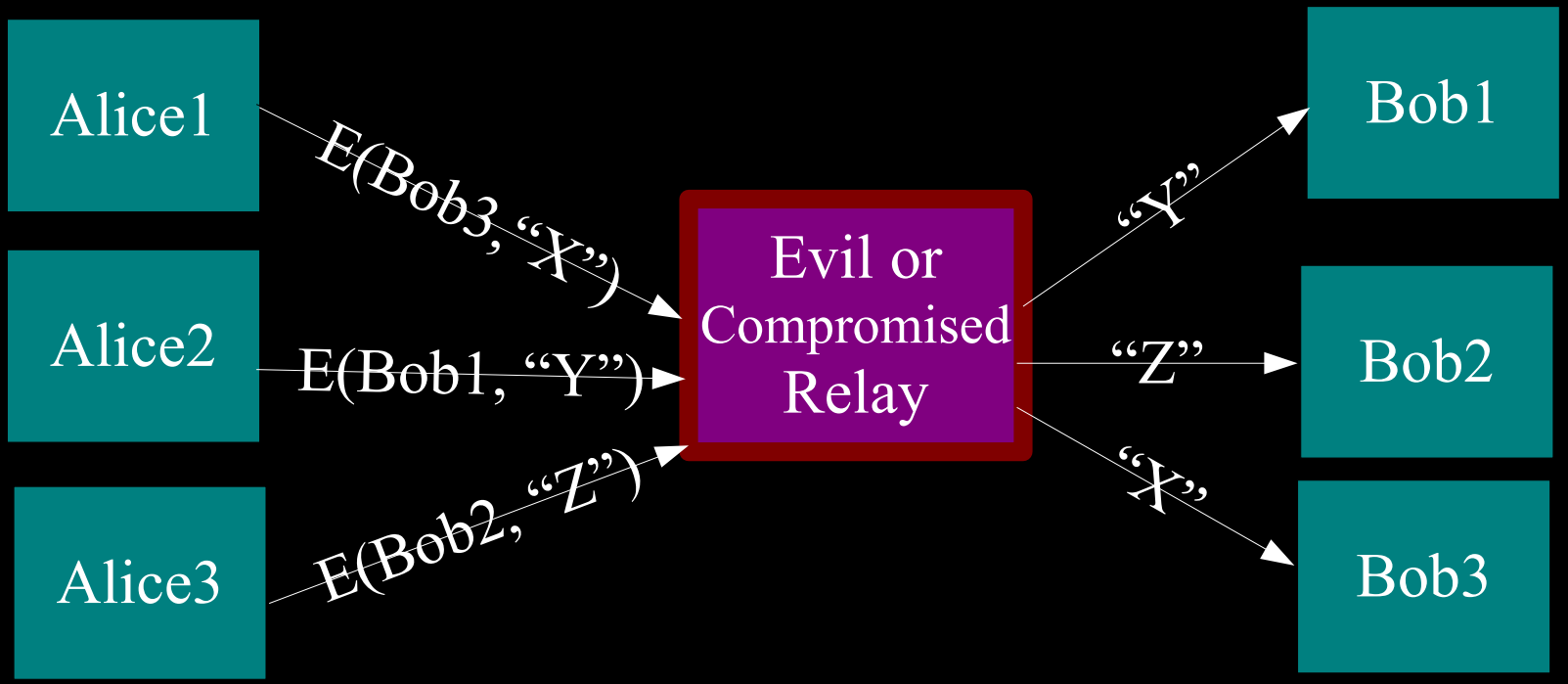


Add encryption to stop attackers who eavesdrop on Alice.

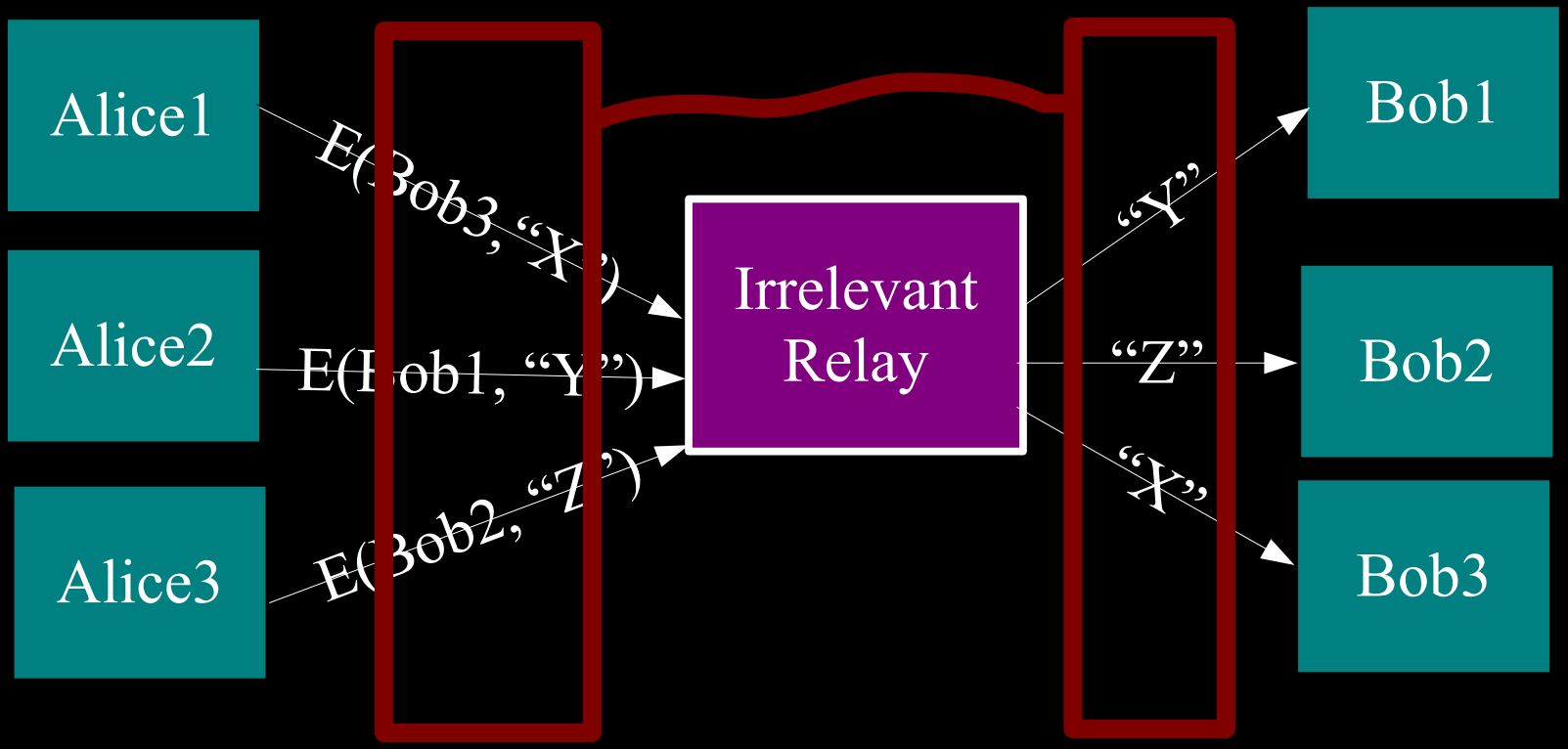


(e.g.: some commercial proxy providers, Anonymizer)

But a single relay is a single point of failure.

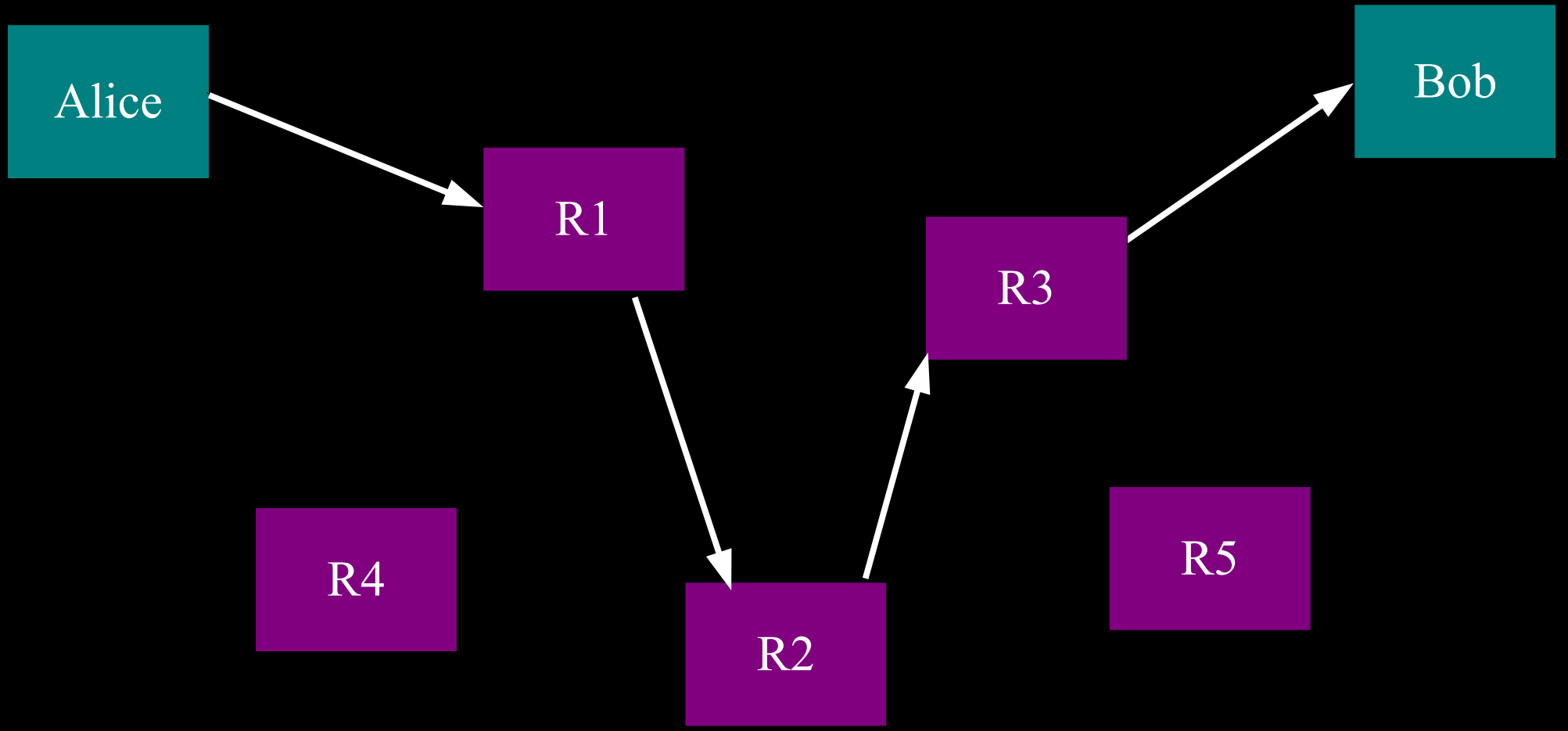


But a single relay is a single point of bypass.

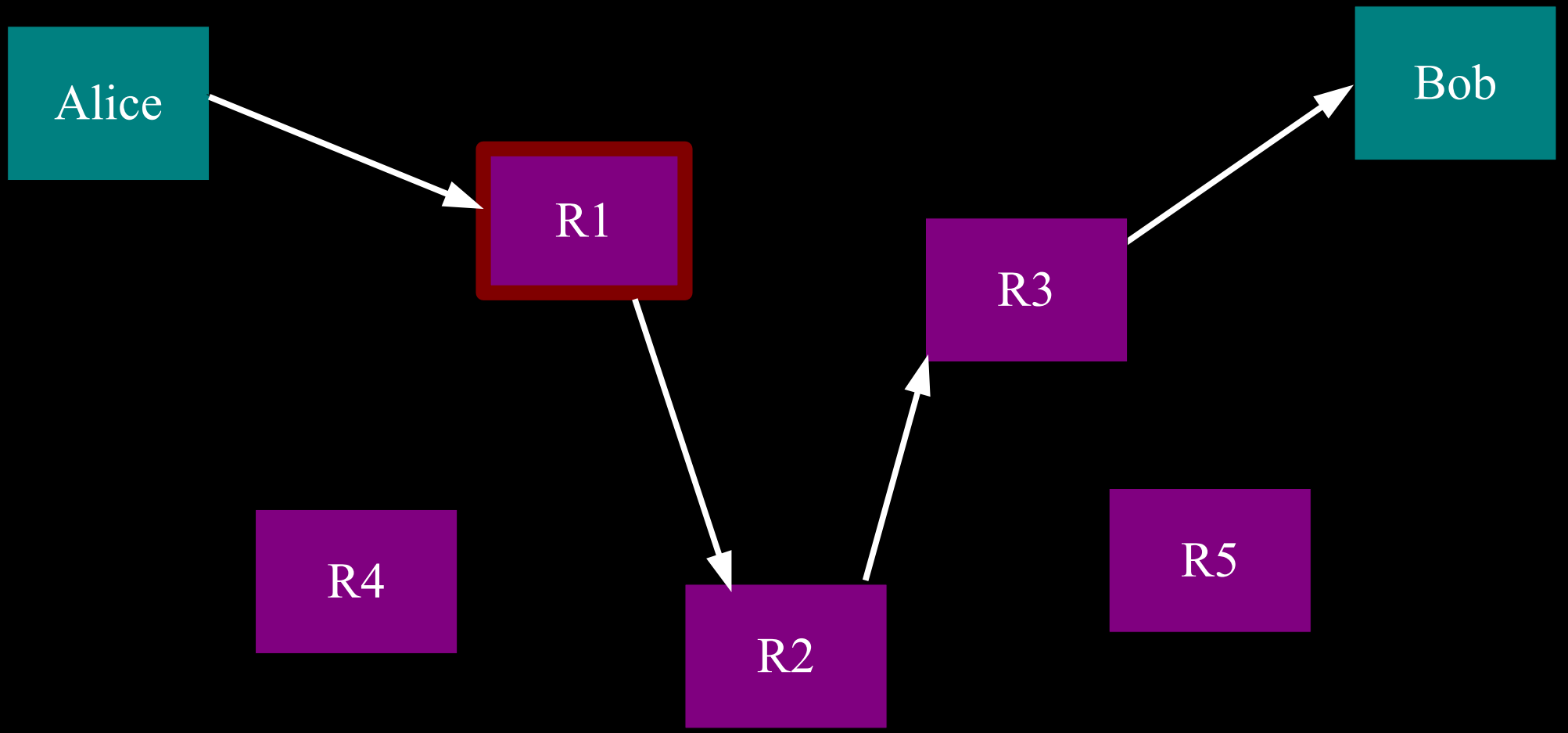


Timing analysis bridges all connections through relay ⇒ An attractive fat target

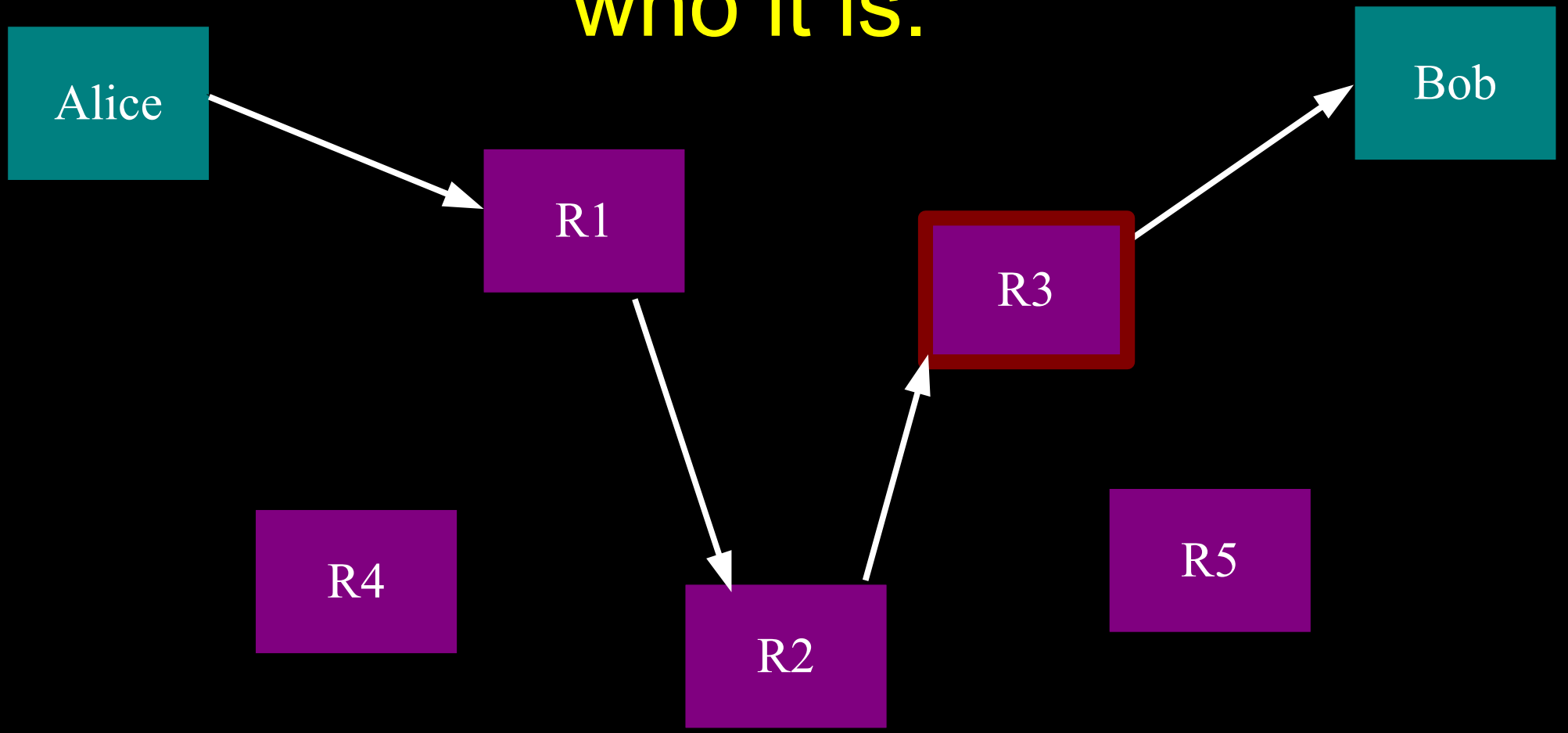
So, add multiple relays so that no single one can betray Alice.



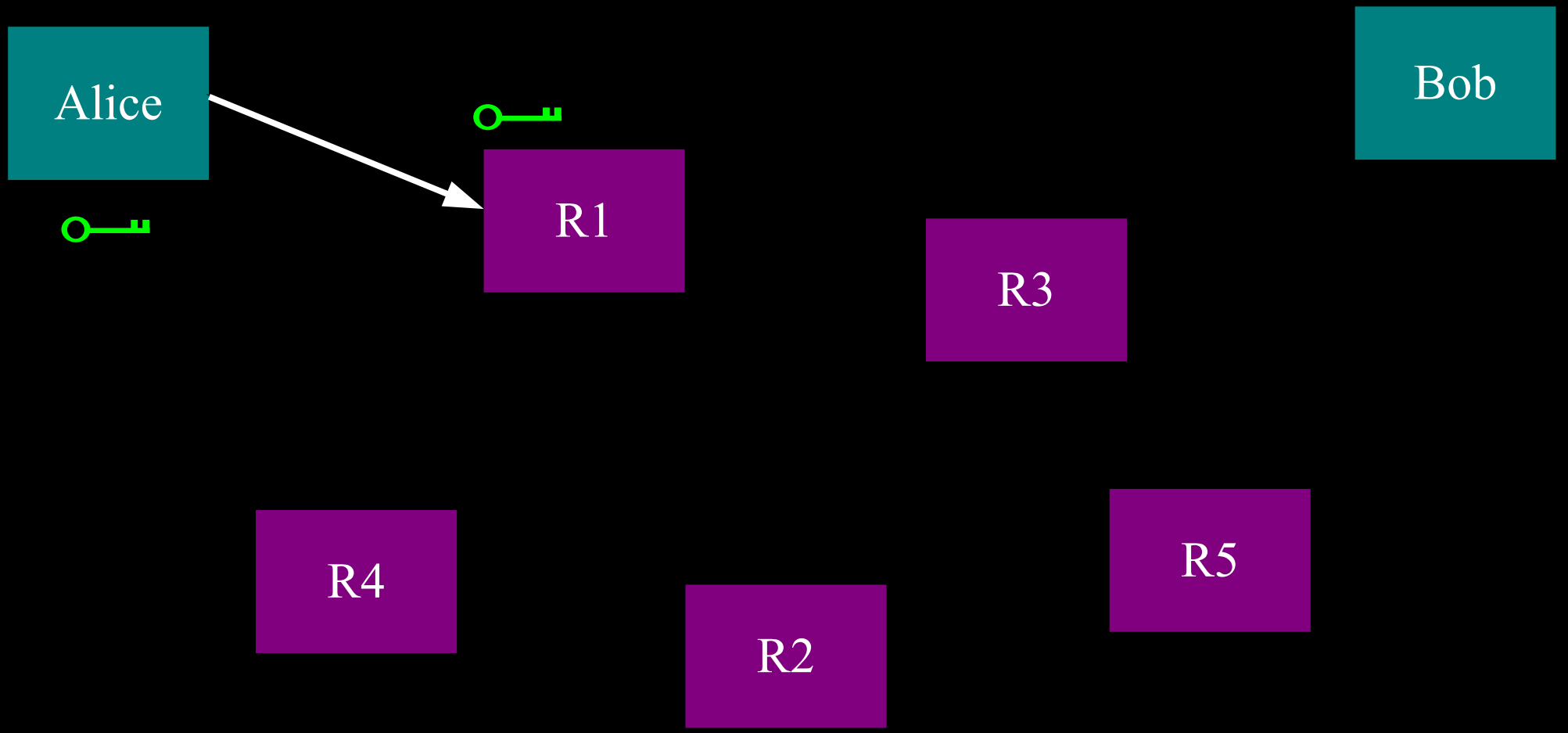
A corrupt first hop can tell that Alice is talking, but not to whom.



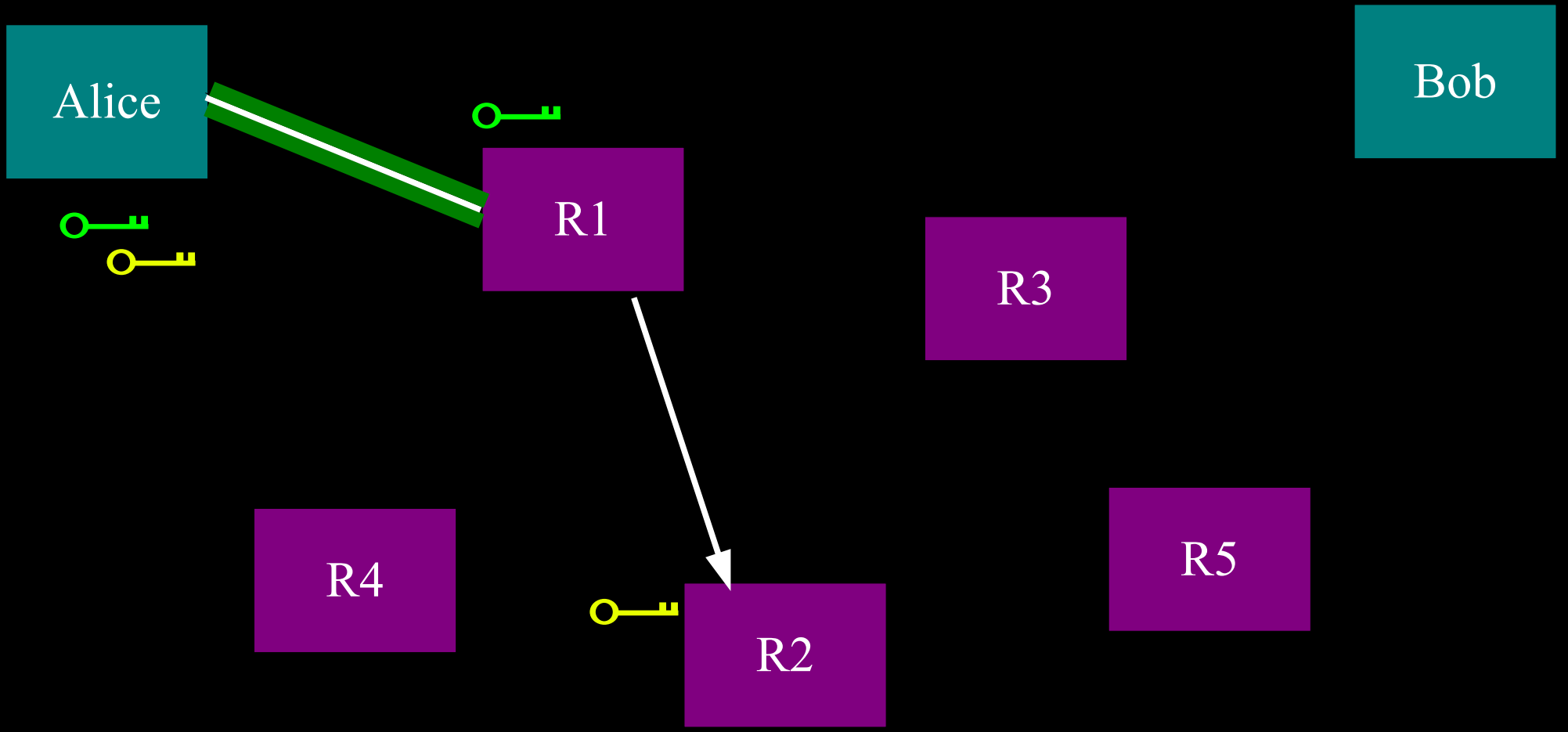
A corrupt final hop can tell someone is talking to Bob, but not who it is.



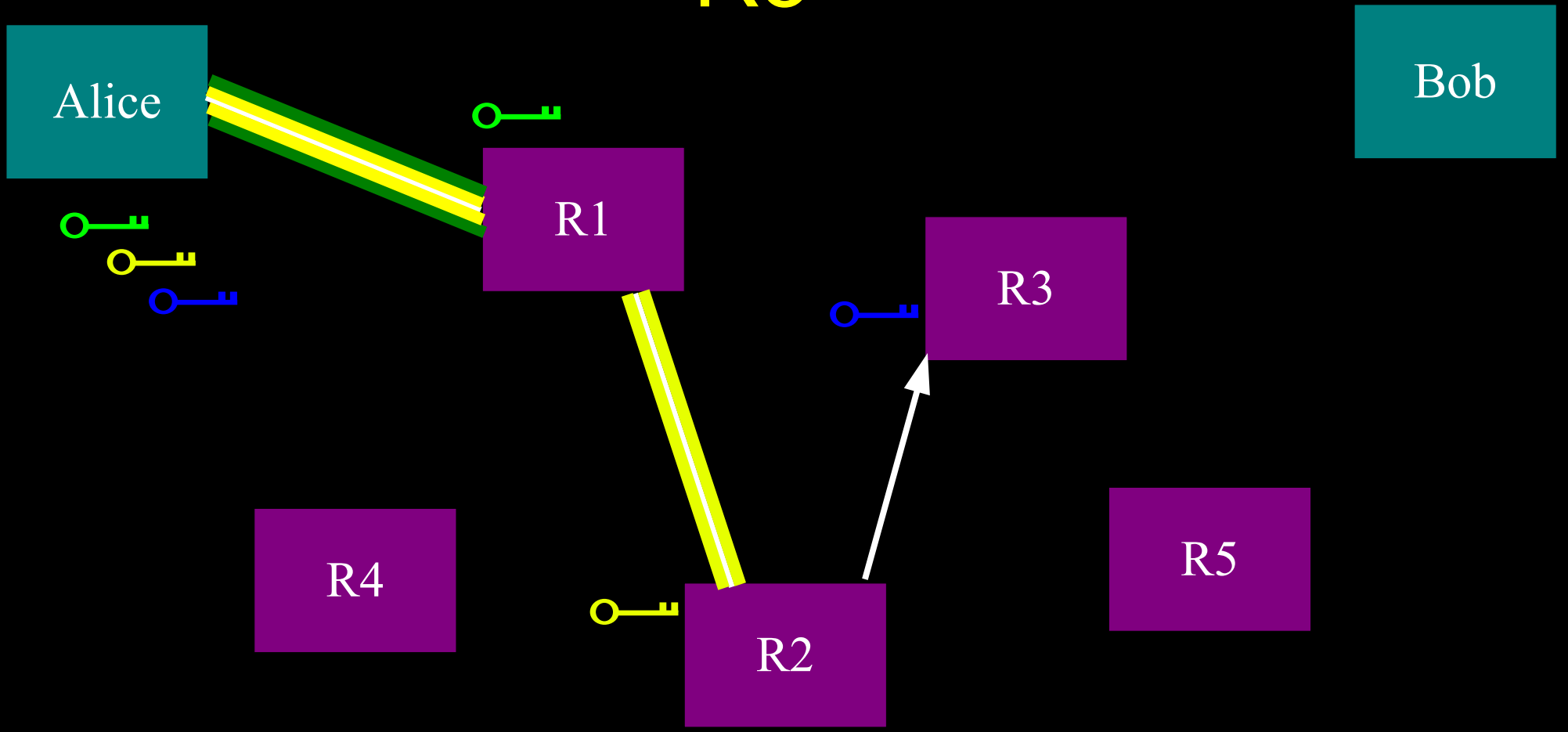
Alice makes a session key with R1



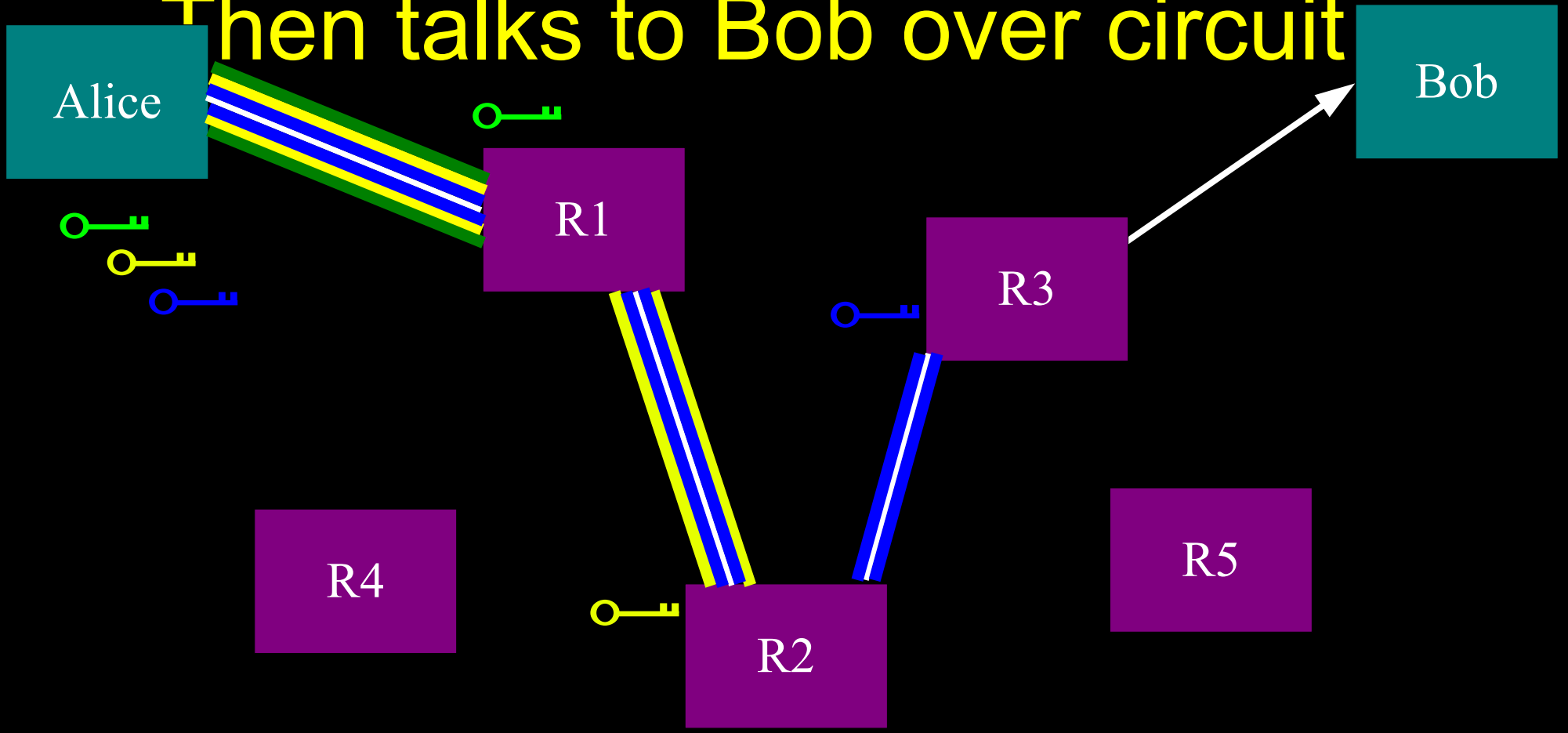
Alice makes a session key with R1 ...And then tunnels to R2



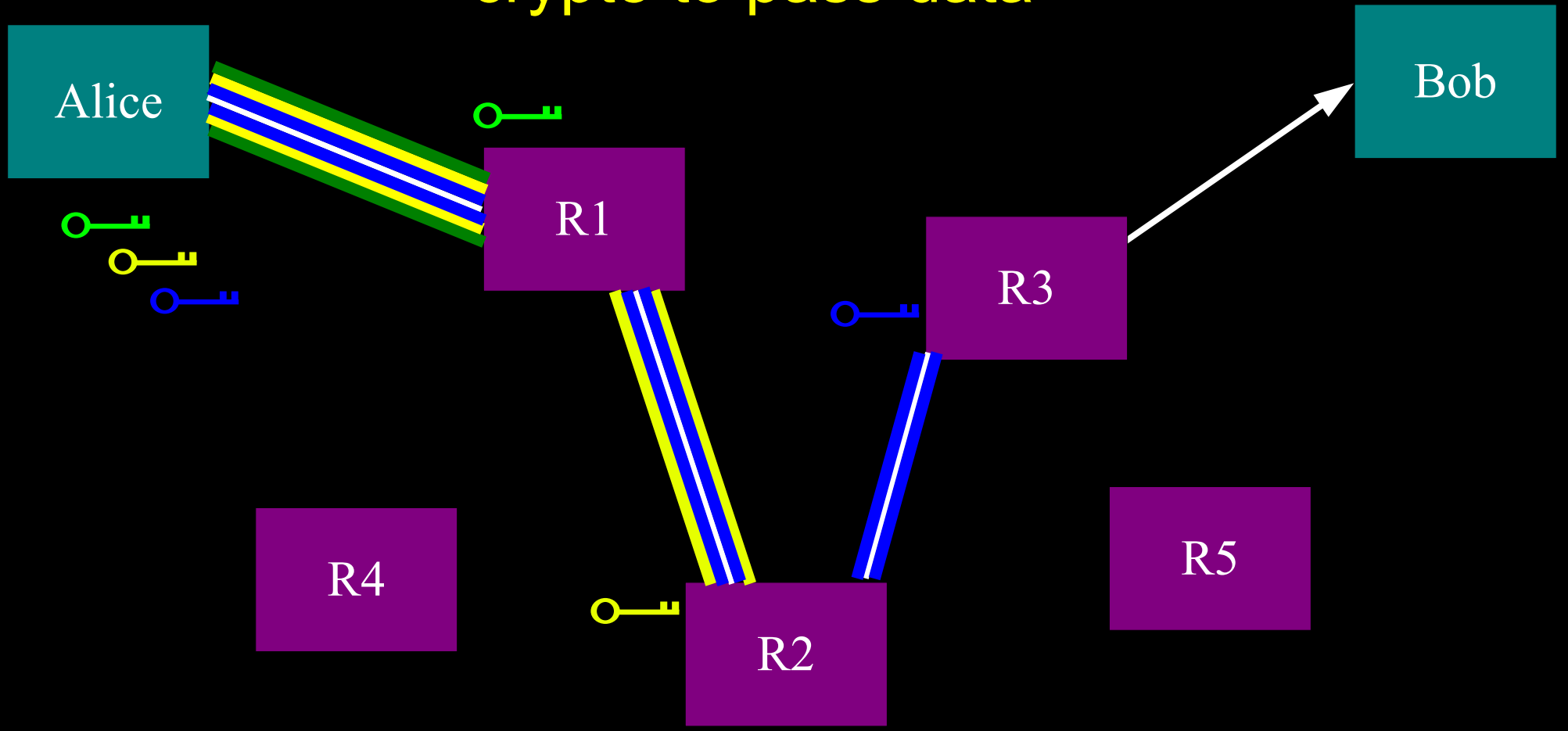
Alice makes a session key with R1 ...And then tunnels to R2...and to R3



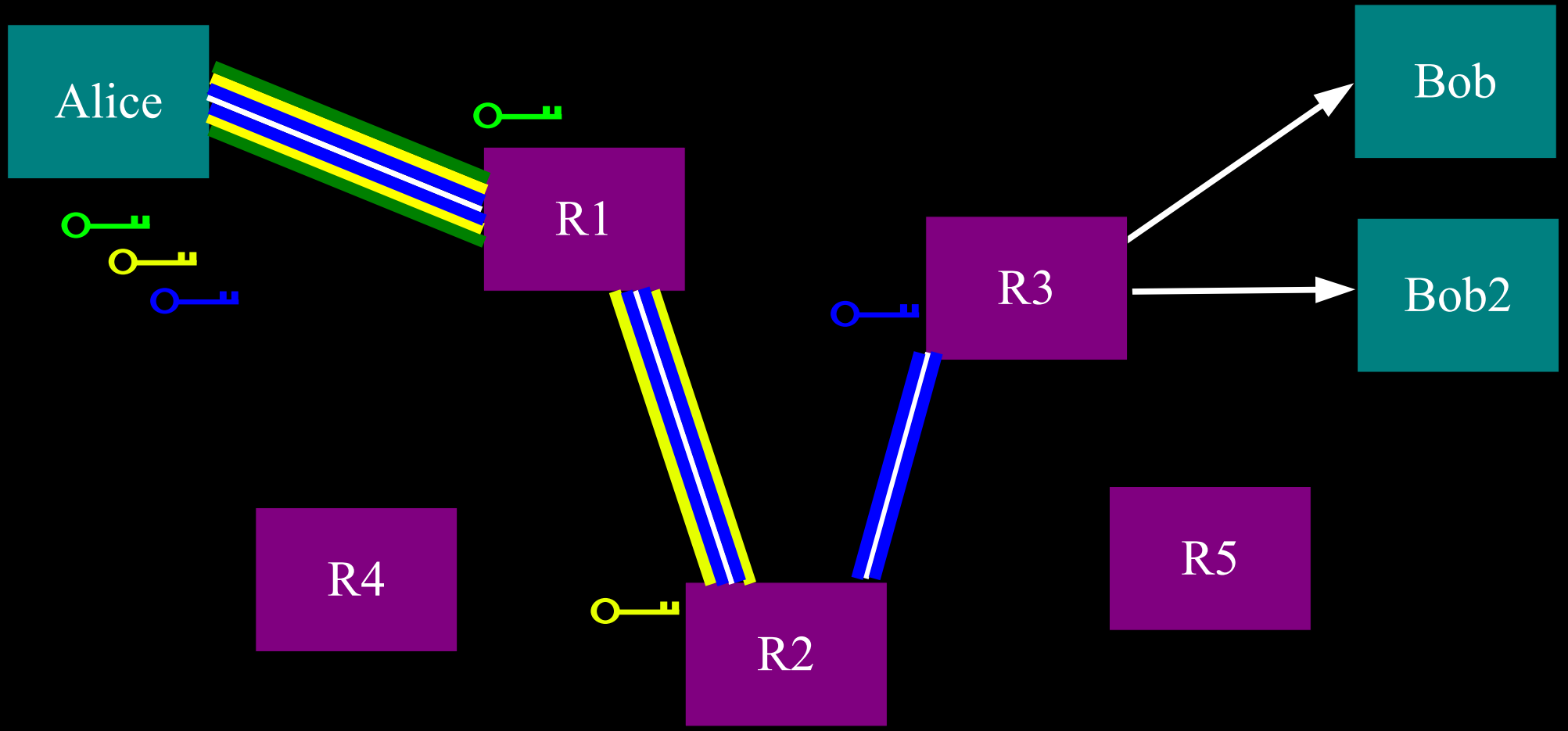
Alice makes a session key with R1 ...And then tunnels to R2...and to R3 Then talks to Bob over circuit



Feasible because onion routing uses (expensive) public-key crypto just to build circuits, then uses (cheaper) symmetric-key crypto to pass data



Can multiplex many connections through the encrypted circuit

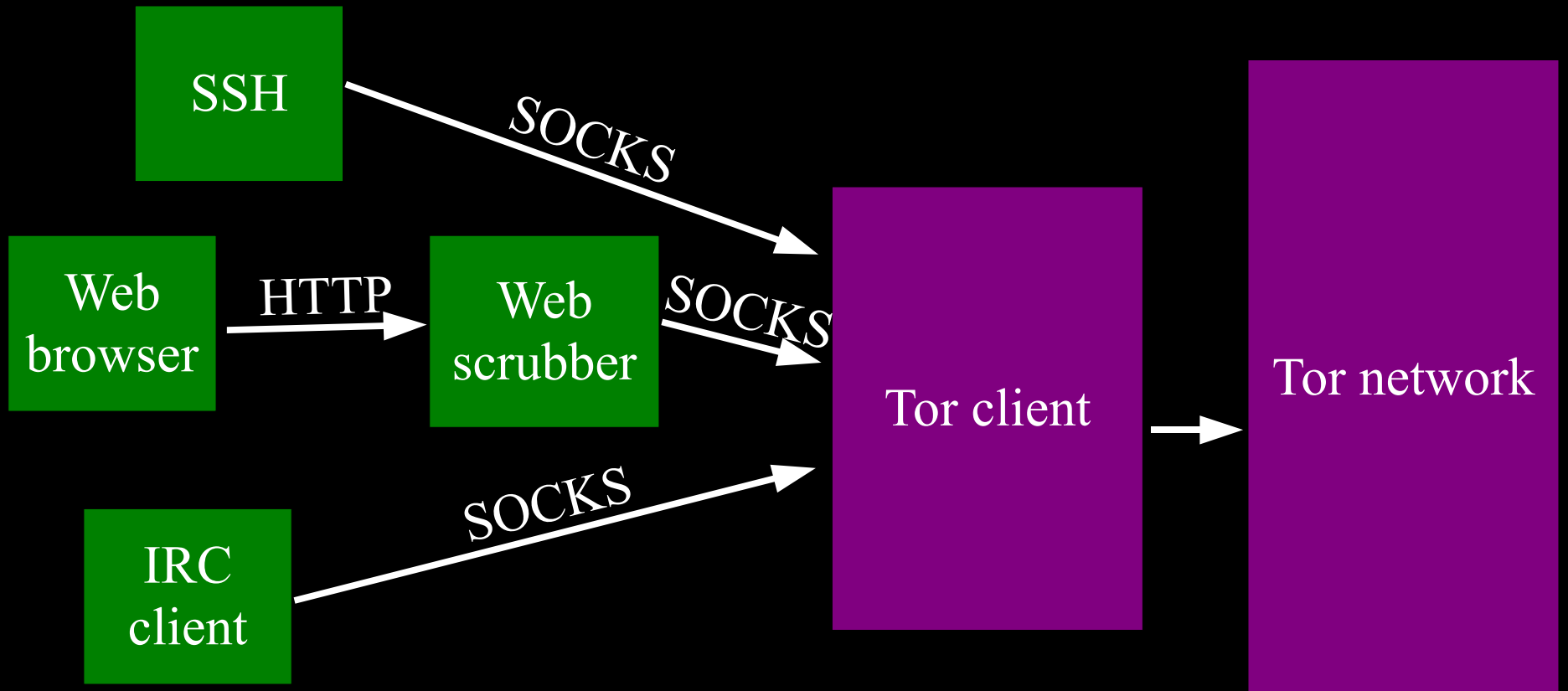


That's Tor* in a nutshell

* Tor's Onion Routing

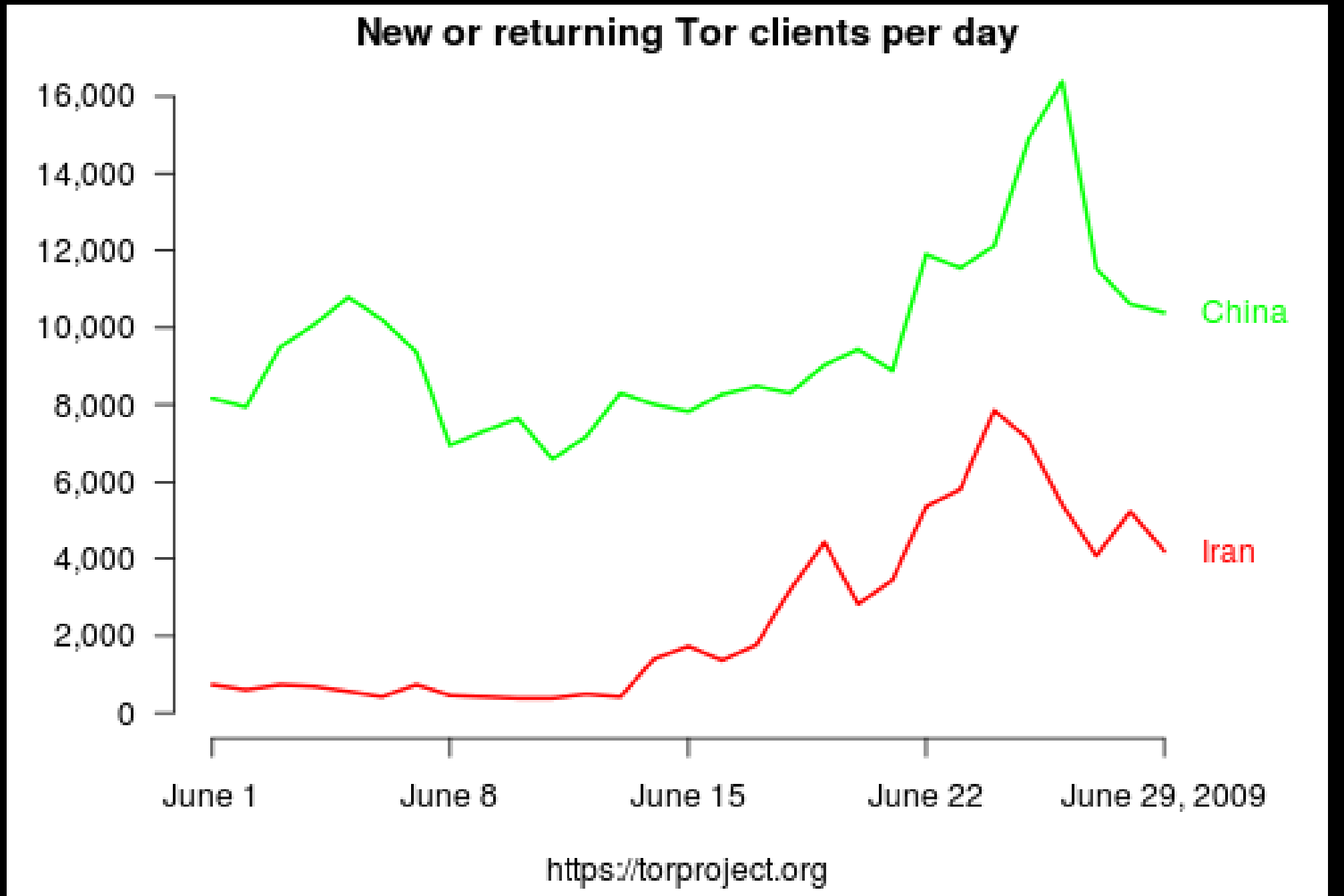
Focus of Tor is anonymity of the communications pipe, not the application data that passes through it

Tor anonymizes TCP streams only: it needs other applications to clean high-level protocols.



Tor: The Big Picture

- Freely available (Open Source), unencumbered, and
- Comes with a spec and full documentation:
  - Docs and instructions translated into 15+ languages
  - German univ. implemented compatible Java Tor clients
  - Researchers use it to study anonymity
- Several commercial imitators
- Focus on Usability/Scalability/Incentives
- 200000+ active users, including various govt. and law enforcement users
- PC World magazine: Tor in the Top 100 Products of 2005.
- Began as NRL research project 2001 (1995)
- Tor Project now a US 501(c) 3 with a handful of employees and many volunteers


New or returning Tor clients per day
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
China
Iran
June 1
June 8
June 15
June 22
June 29, 2009
https://torproject.org

Usability for relay operators

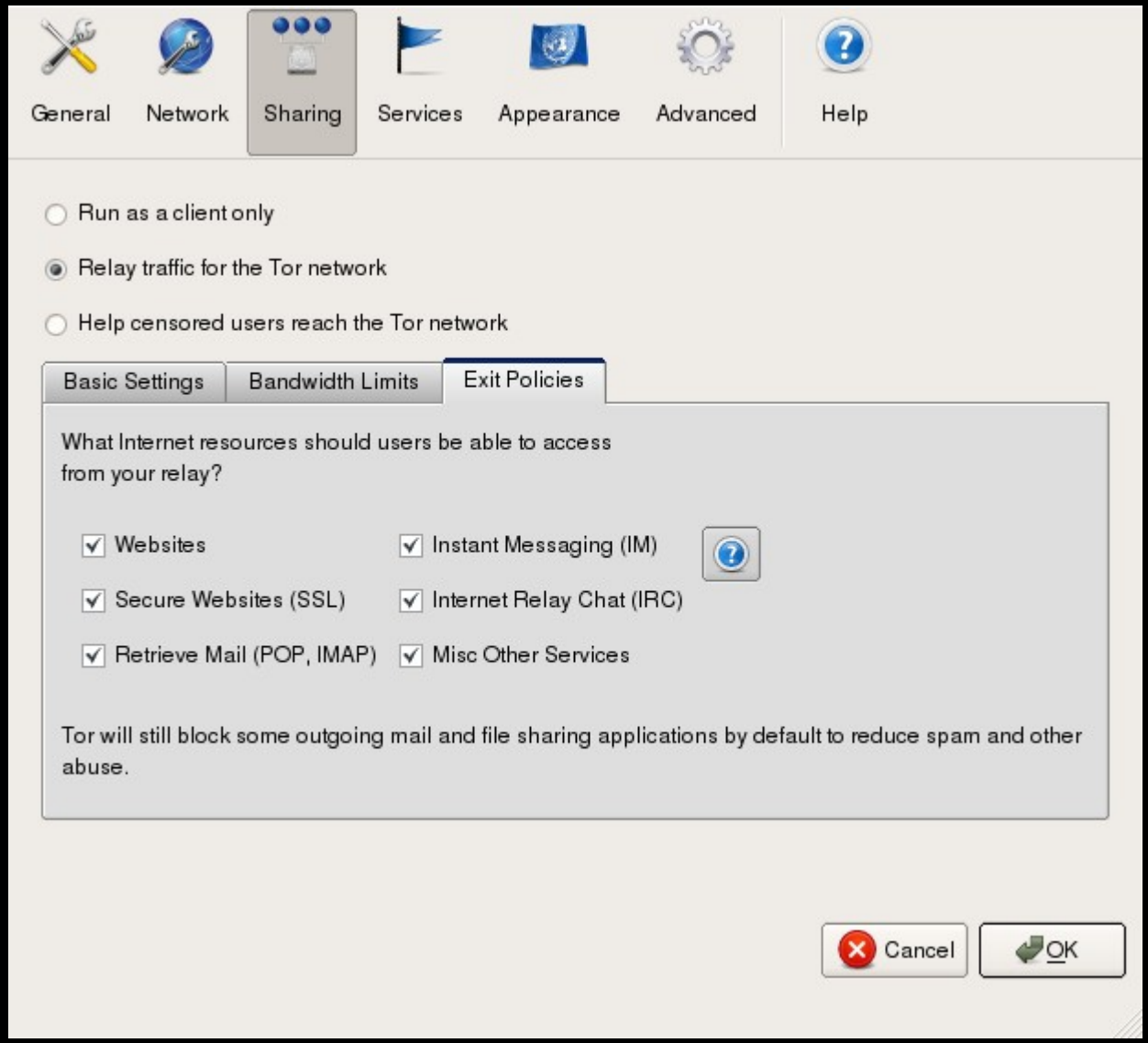
- Rate limiting: shouldn't eating too much bandwidth.
- Exit policies: not everyone is willing to emit arbitrary traffic.

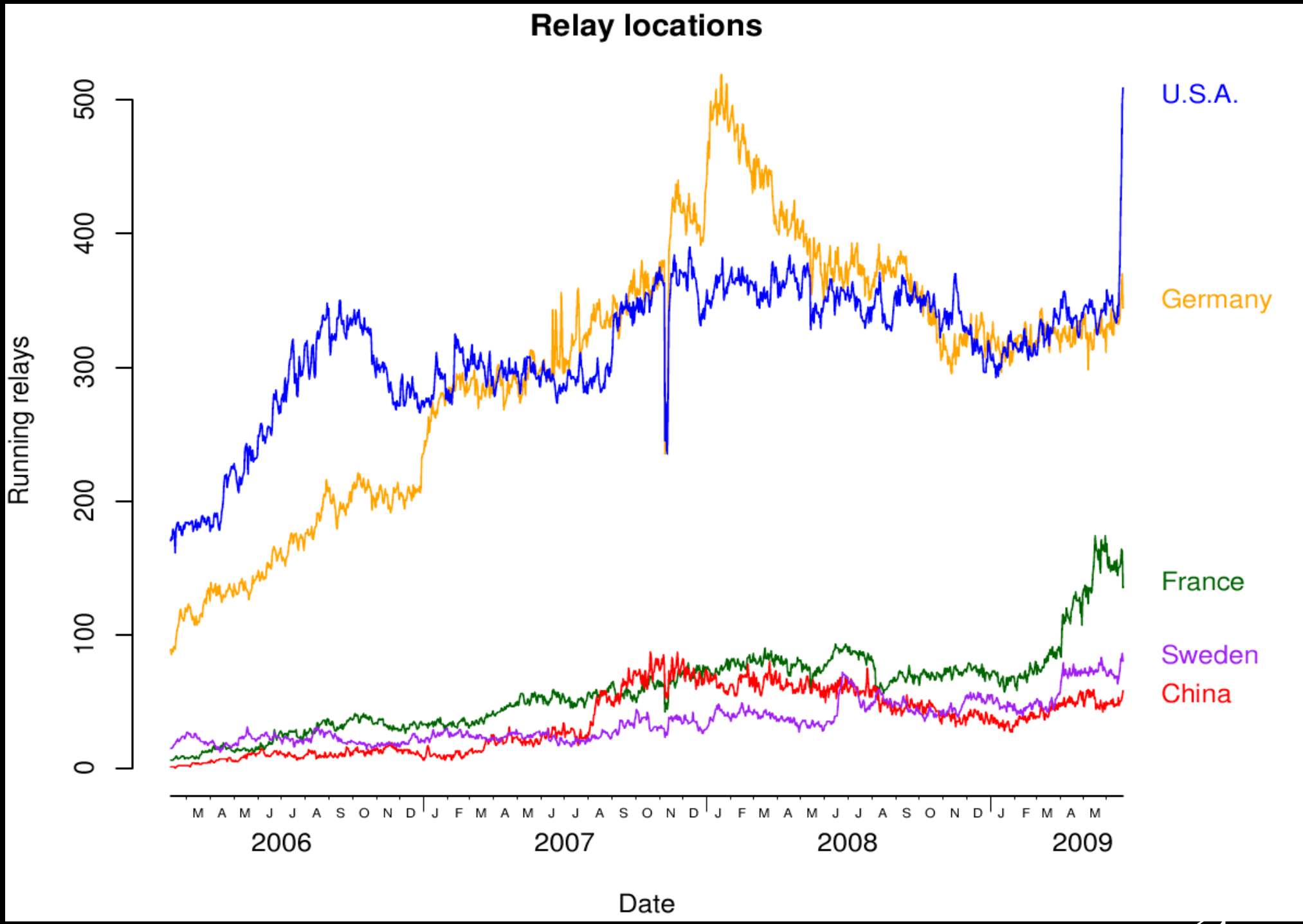
```
allow 18.0.0.0/8:*
    allow *:22
    allow *:80
    reject *:*
```

- Middle-man node: no exit from Tor network (reject *:*)
- Bridge node: not part of public Tor network at all

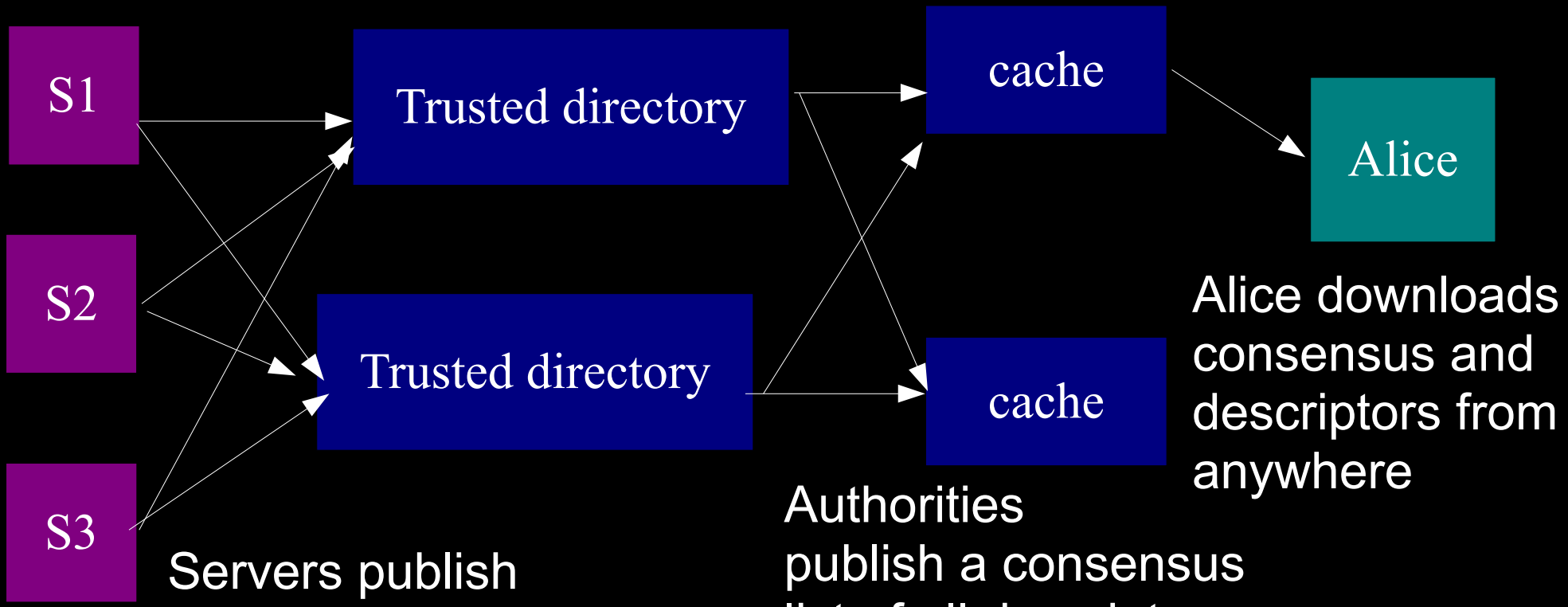
Choose how to install it

- Tor Browser Bundle: standalone Windows exe with Tor, Vidalia, Firefox, Torbutton, Polipo, e.g. for USB stick
- Vidalia bundle: Windows/OSX installer
- Tor VM: Transparent proxy for Windows
- “Net installer” via our secure updater
- Incognito Linux LiveCD

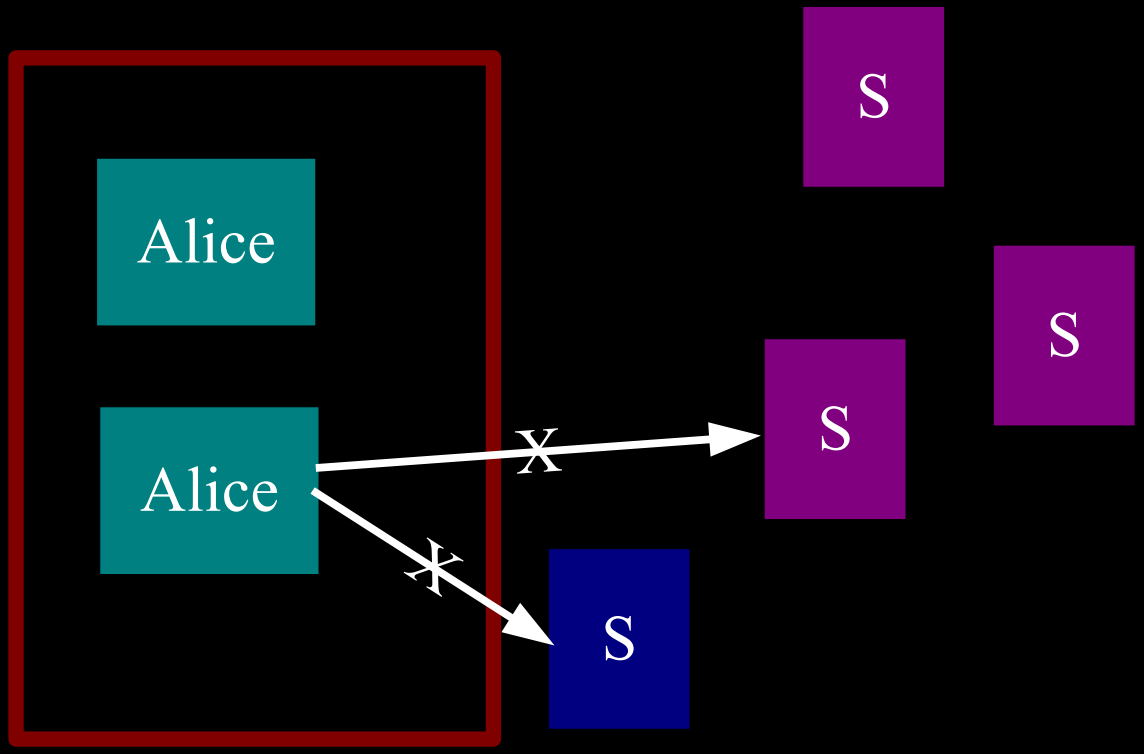

General
Network
Sharing
Services
Appearance
Advanced
Help
Run as a client only
Relay traffic for the Tor network
Help censored users reach the Tor network
Basic Settings
Bandwidth Limits
Exit Policies
What Internet resources should users be able to access from your relay?
Websites
Instant Messaging (IM)
Secure Websites (SSL)
Internet Relay Chat (IRC)
Retrieve Mail (POP, IMAP)
Misc Other Services
Tor will still block some outgoing mail and file sharing applications by default to reduce spam and other abuse.
Cancel
OK

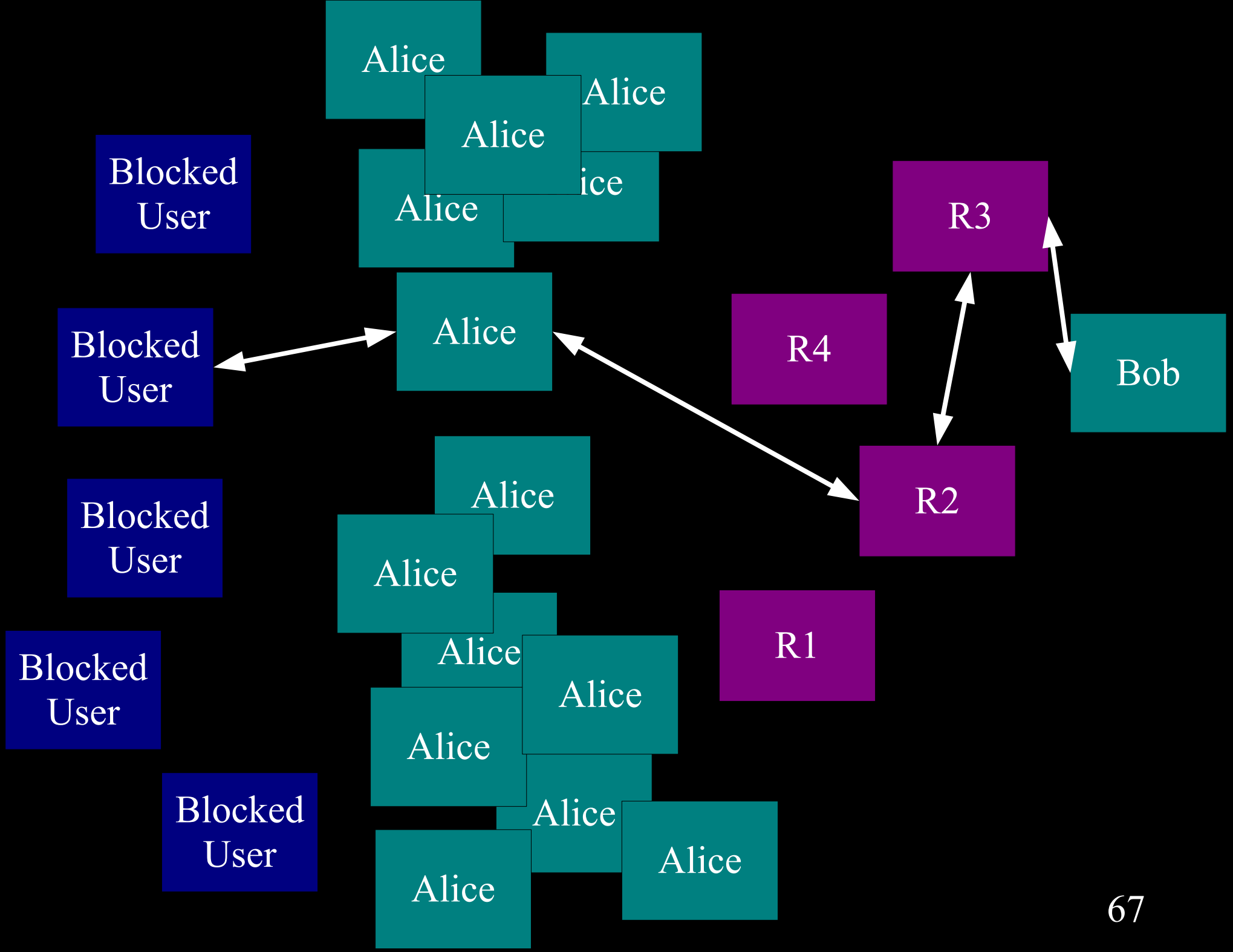

Relay locations
Running relays
0
100
200
300
400
500
U.S.A.
Germany
France
Sweden
China
M A M J J A S O N D J F M A M J J A S O N D J F M A M J J A S O N D J F M A M
2006
2007
2008
2009
Date

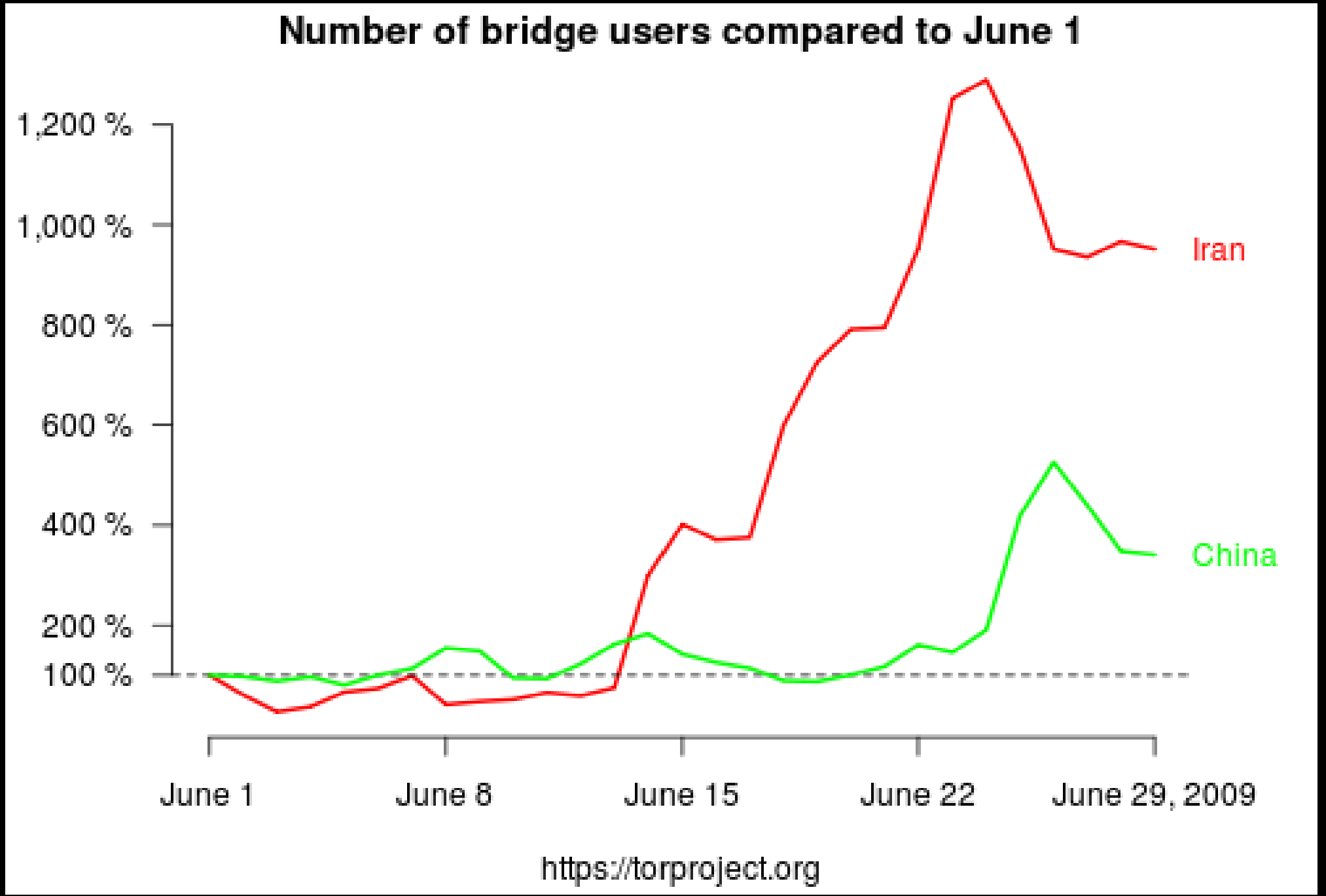
The basic Tor design uses a simple centralized directory protocol.



Governments and other firewalls can just block the whole Tor network.




Alice
Alice
Alice
Alice
ice
Blocked User
R3
Alice
R4
Blocked User
Bob
Alice
R2
Blocked User
Alice
Alice
Alice
R1
Blocked User
Alice
Alice
Alice
Blocked User
Alice
Alice


Number of bridge users compared to June 1
1,200 %
1,000 %
800 %
600 %
400 %
200 %
100 %
Iran
China
June 1
June 8
June 15
June 22
June 29, 2009
https://torproject.org

Tor is only a piece of the puzzle

- Assume the users aren't attacked by their hardware and software
  - No spyware installed, no cameras watching their screens, etc
- Assume the users can fetch a genuine copy of Tor: from a friend, via PGP signatures, etc.

Lessons?

- 1) Bad people don't need Tor. They're doing fine.
- 2) Honest people need more security/privacy/anonymity.
- 3) Law enforcement can benefit from it too.
- 4) Tor is not unbreakable.

Suggestions: Know your adversary

- Destination adversary: lock down applications, etc. https://www.torproject.org/download.html/#Warning
- Exit node adversary: same advice, also worry about pseudonymous profiles.
  - DON'T assume passwords over otherwise unencrypted links are safe because they went through Tor first.
- Local/temporary adversary: you are probably OK just using (properly configured) Tor
  - CAVEAT: You might have other adversaries watching you even if they are not your immediate concern

Suggestions: Know your adversary

- Well-funded tech-savvy adversary: Be patient, onion routing is not there yet.
  - Using Tor is usually better than not using Tor or using anything else I know of.
  - Nothing to prevent someone from running a nontrivial percentage of Tor nodes and watching the traffic over them and/or watching internet connections.
  - Currently working on research to work trust into the model and design of Tor.

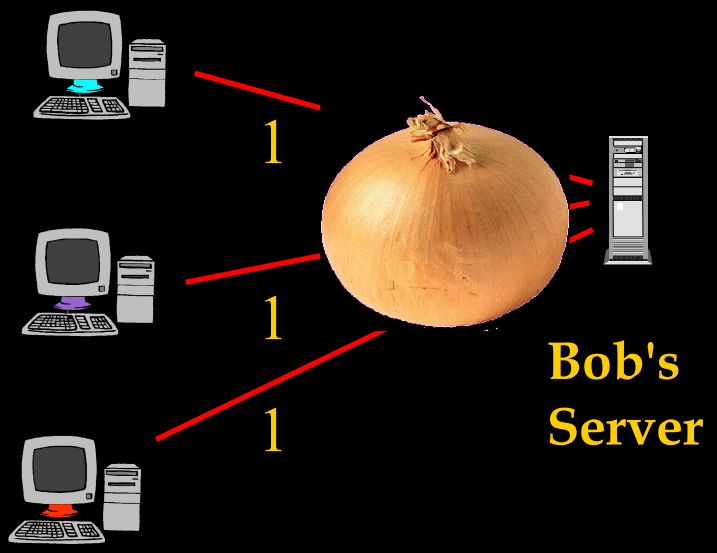
Location Hidden Servers

- Alice can connect to Bob's server without knowing where it is or possibly who he is
- Already told you why this is desirable, but...
-
- How is this possible?

Location Hidden Servers

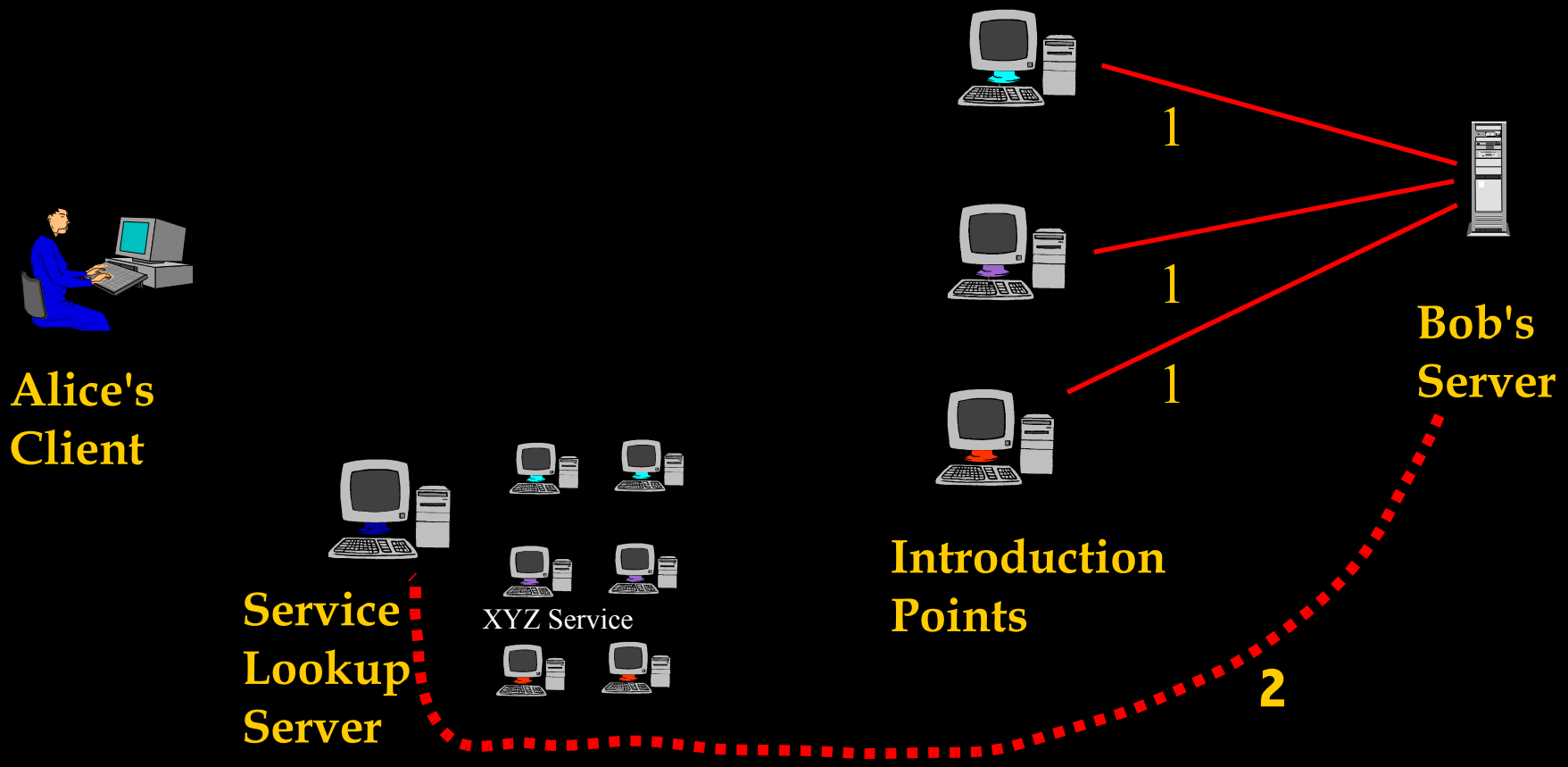
1. Server Bob creates onion routes to Introduction Points (IP)

   (All routes in these pictures are onion routed through Tor)



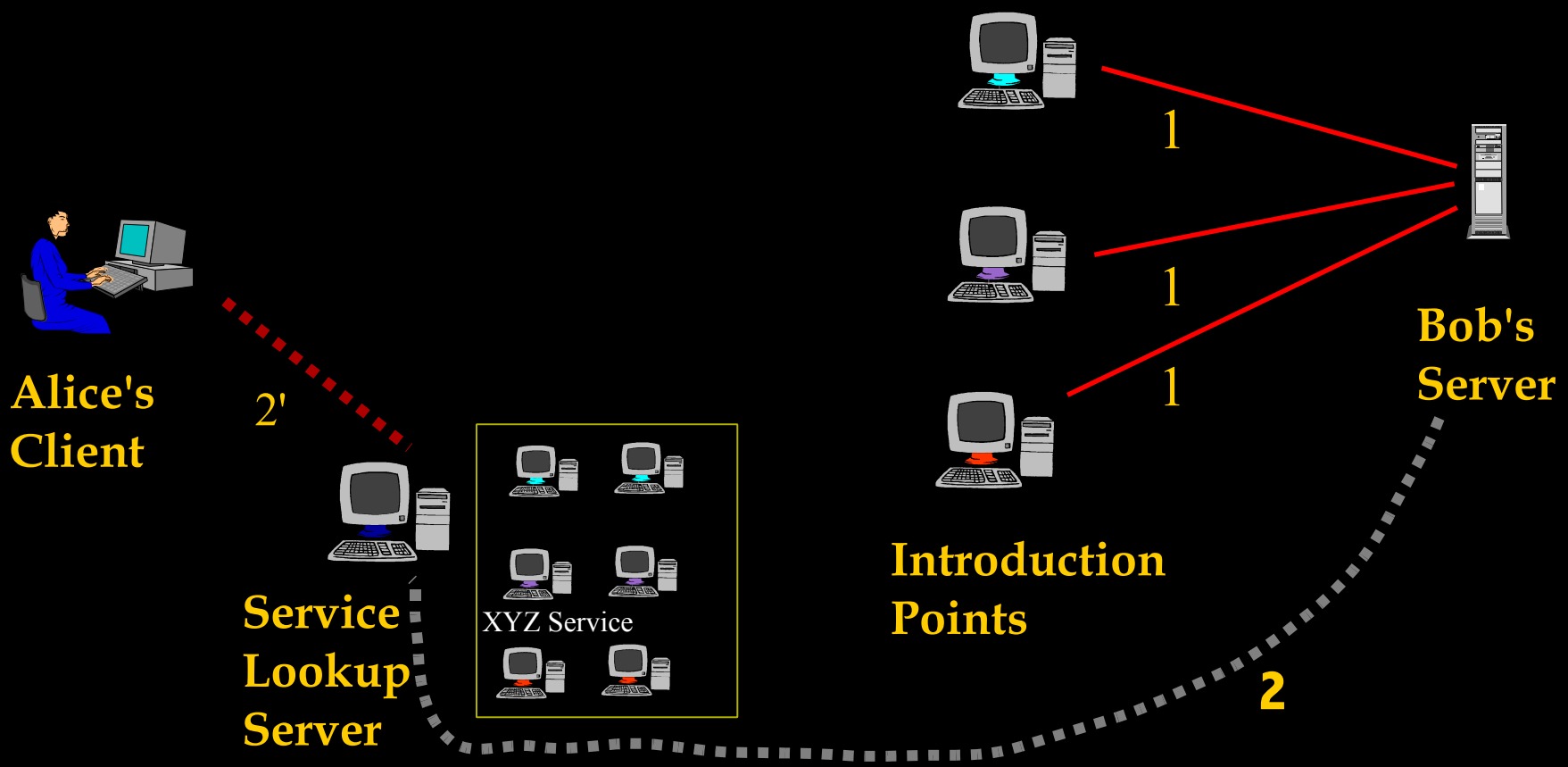
Location Hidden Servers

1. Server Bob creates onion routes to Introduction Points (IP)
2. Bob publishes his xyz.onion address and puts Service Descriptor incl. Intro Pt. listed under xyz.onion



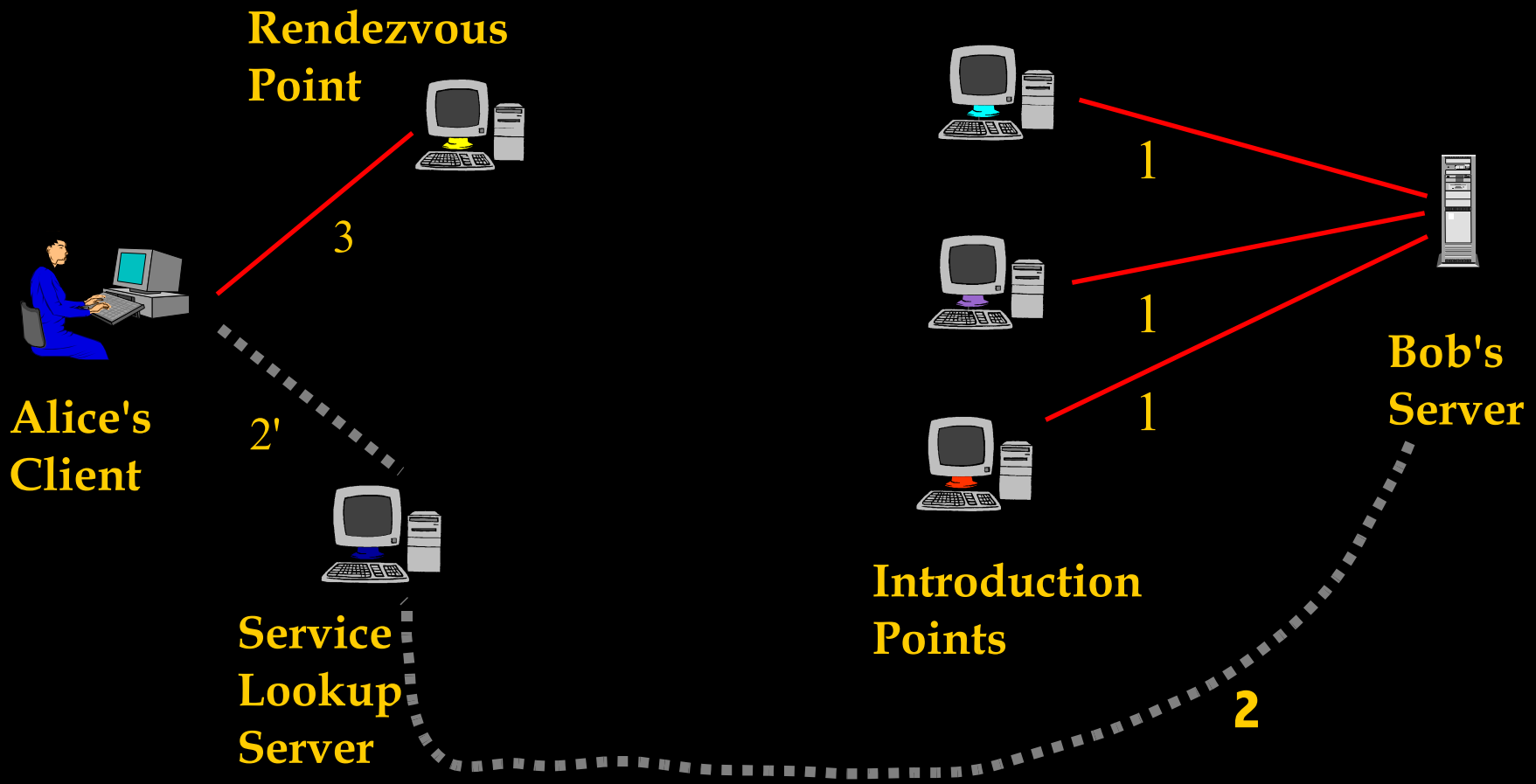
Location Hidden Servers

2'. Alice uses xyz.onion to get Service Descriptor (including Intro Pt. address) at Lookup Server



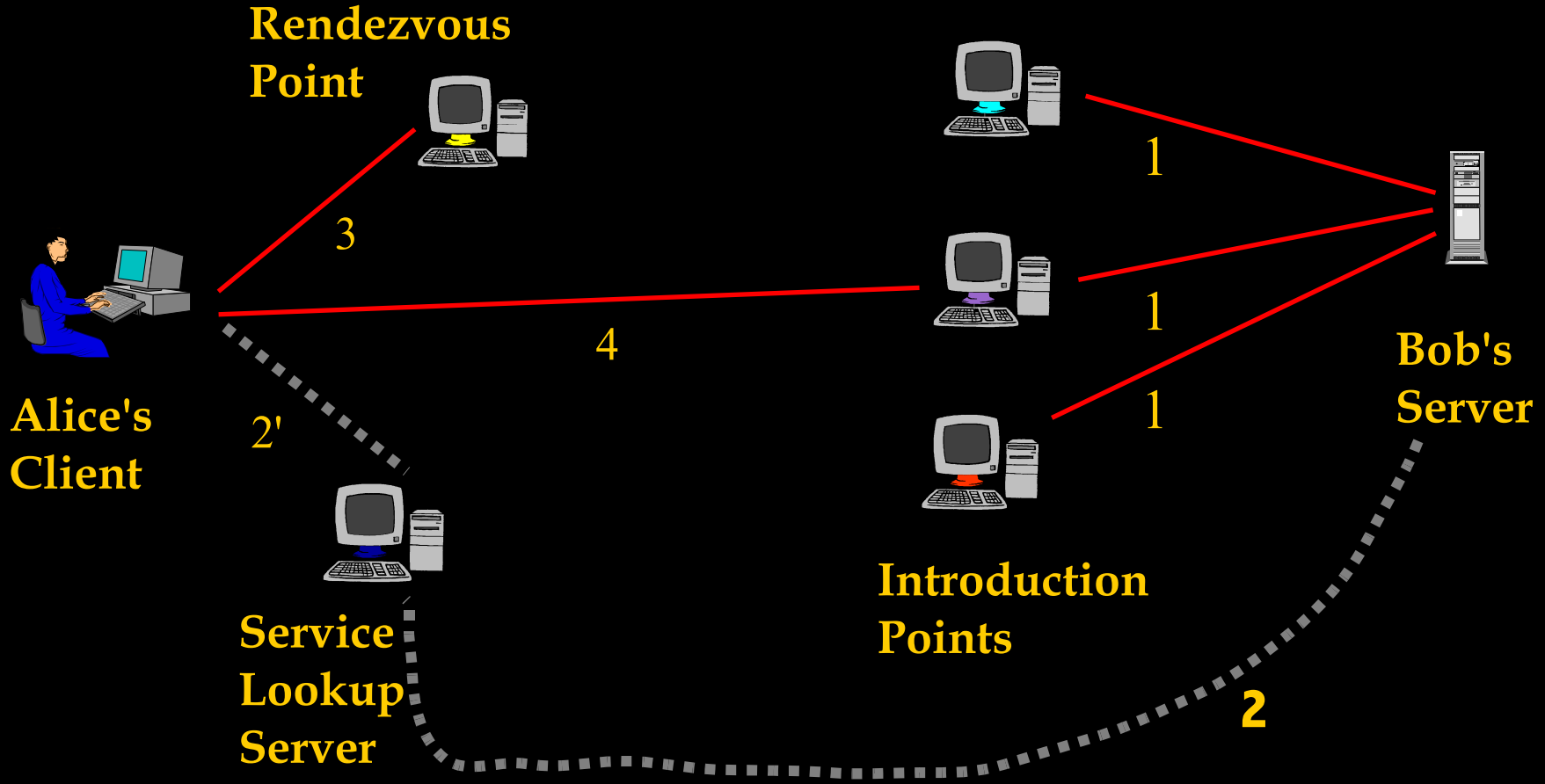
Location Hidden Servers

3. Client Alice creates onion route to Rendezvous Point (RP)



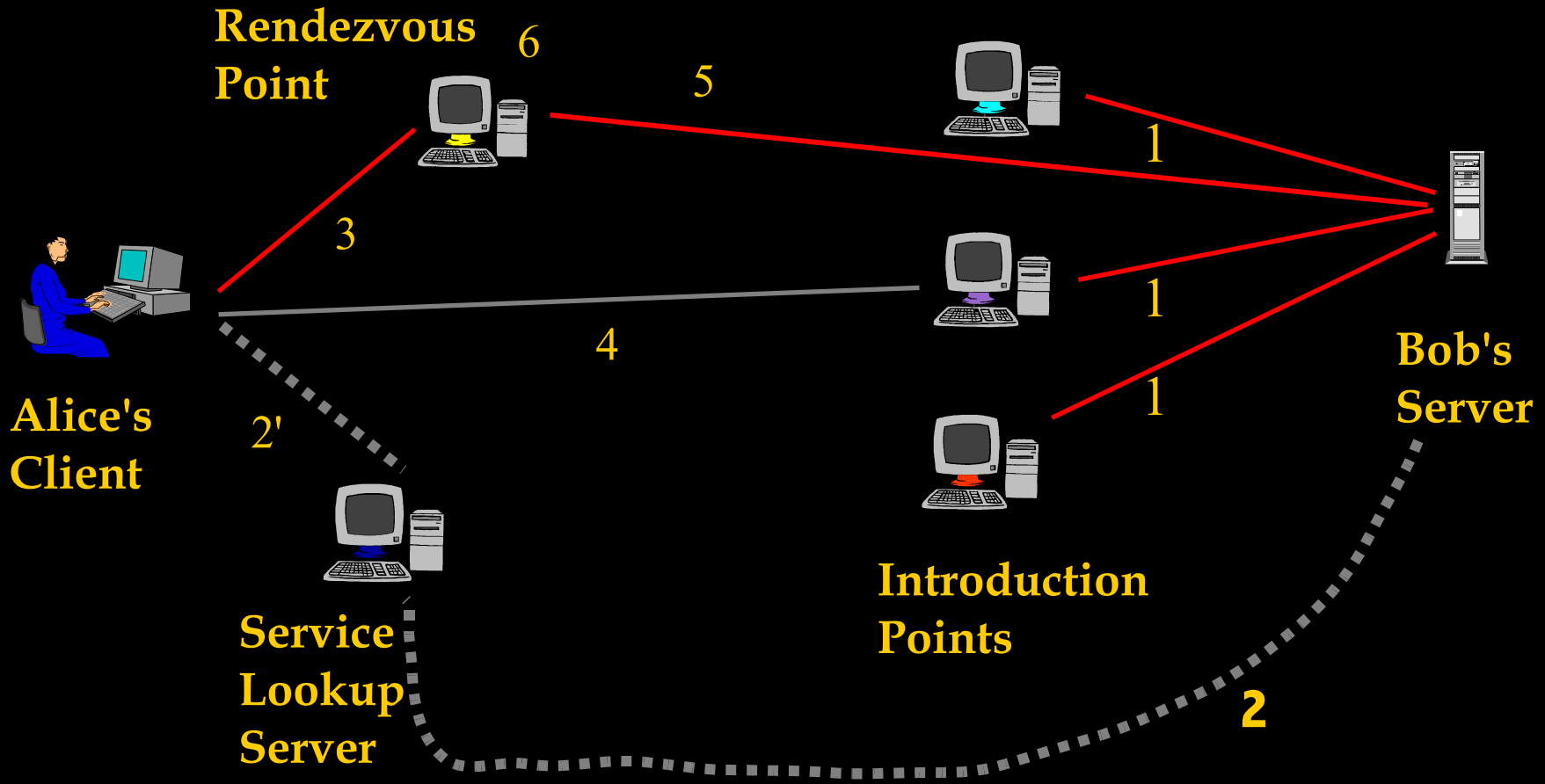
Location Hidden Servers

3. Client Alice creates onion route to Rendezvous Point (RP)
4. Alice sends RP address and any authorization through IP to Bob



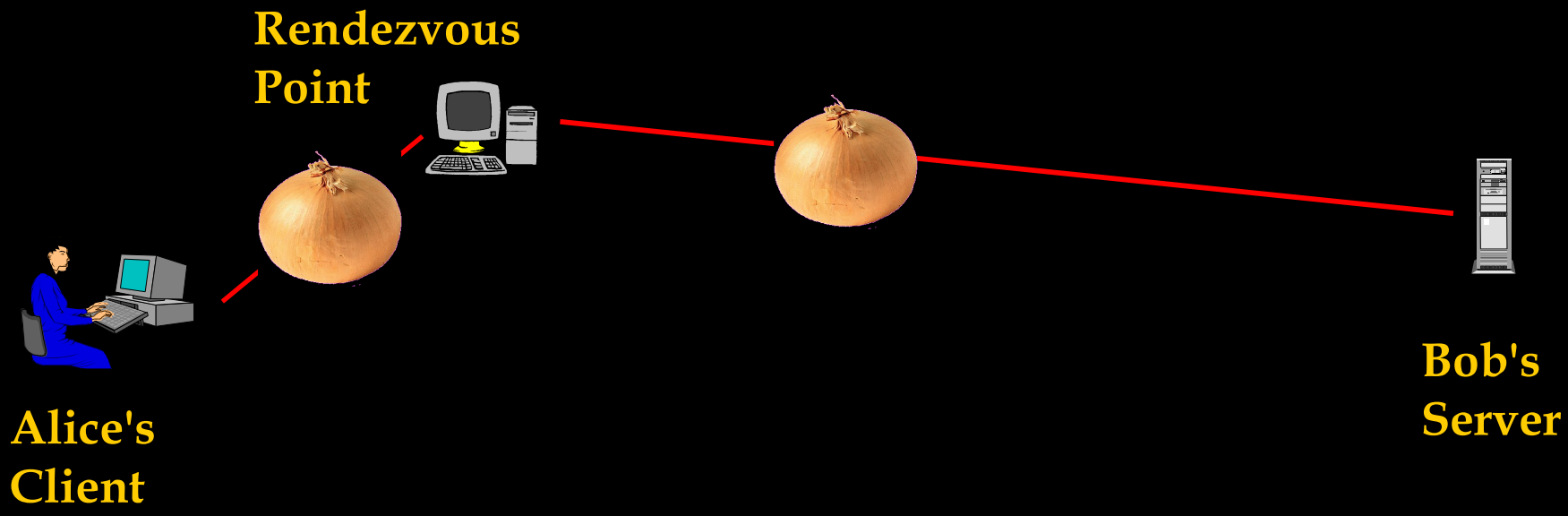
Location Hidden Servers

5. If Bob chooses to talk to Alice, connects to Rendezvous Point
6. Rendezvous Point mates the circuits from Alice and Bob



Location Hidden Servers

Final resulting communication channel



Further Questions?

- Contact me:
  http://www.syverson.org
- Onion Routing homepage:
  http://www.onion-router.net
- Download/read about Tor:
  https://www.torproject.org
- Major papers on anonymity:
  htttp://freehaven.net/anonbib