A Peel of Onion

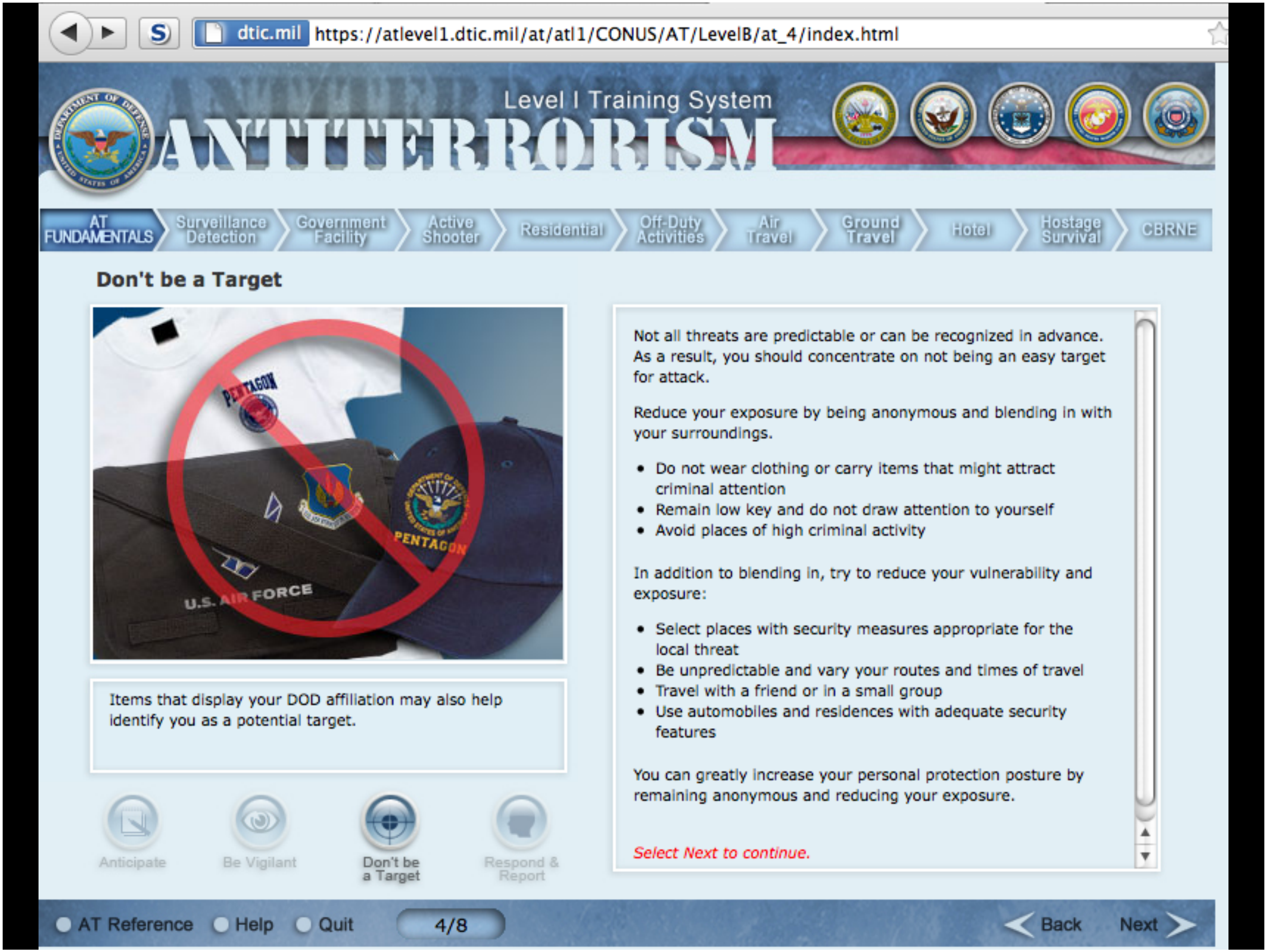
Paul Syverson
U.S. Naval Research Laboratory
syverson@itd.nrl.navy.mil
http://www.syverson.org

“Our motivation here is not to provide anonymous communication, but to separate identification from routing.”

- “Proxies for anonymous routing”. Reed, Syverson, and Goldschlag. ACSAC 1996

A Motivational Use Case Example

- Navy Petty Officer Alice is temporarily in Repressia



Don't be a Target

Items that display your DOD affiliation may also help identify you as a potential target.

Not all threats are predictable or can be recognized in advance. As a result, you should concentrate on not being an easy target for attack.

Reduce your exposure by being anonymous and blending in with your surroundings.

- Do not wear clothing or carry items that might attract criminal attention
- Remain low key and do not draw attention to yourself
- Avoid places of high criminal activity

In addition to blending in, try to reduce your vulnerability and exposure:

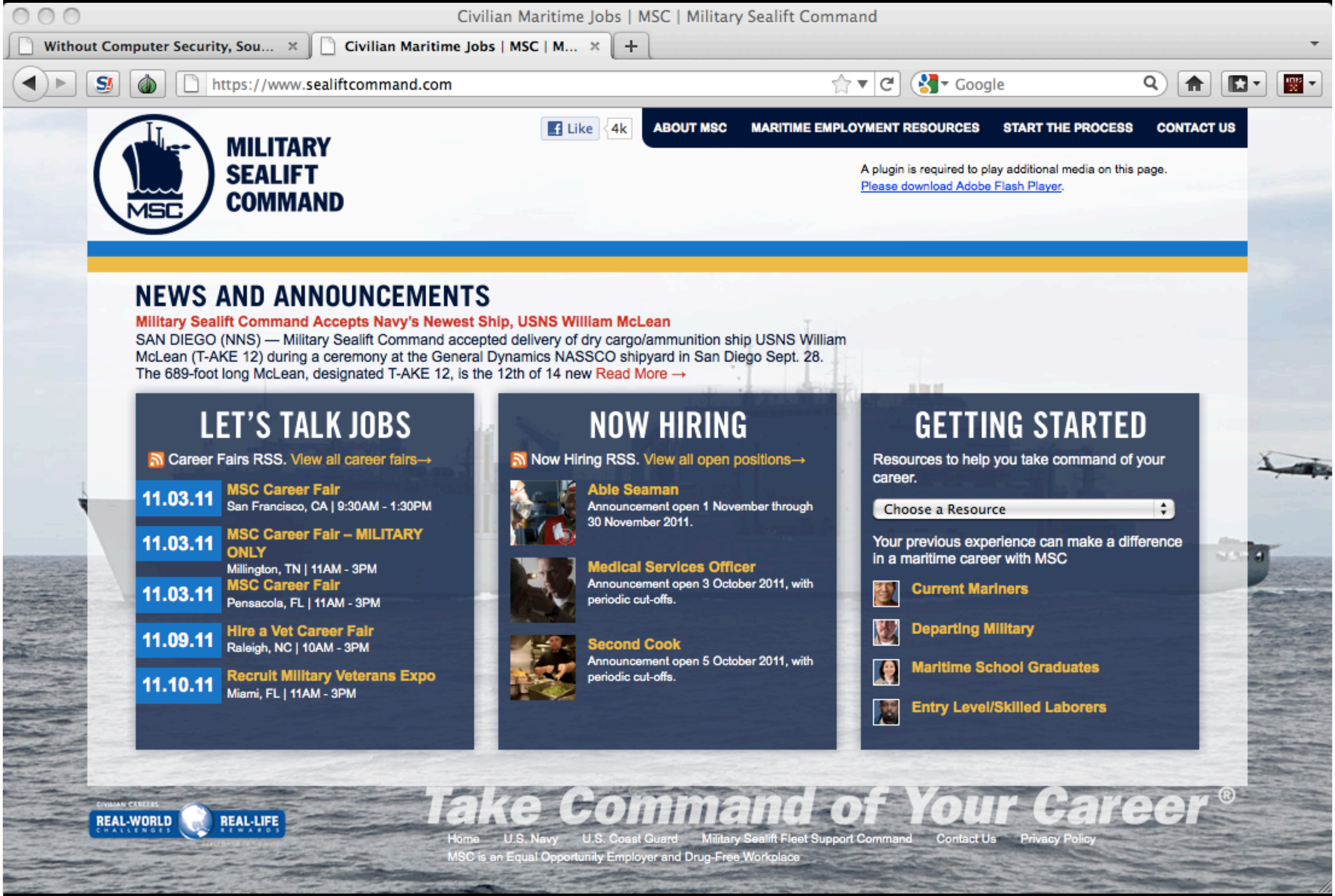
- Select places with security measures appropriate for the local threat
- Be unpredictable and vary your routes and times of travel
- Travel with a friend or in a small group
- Use automobiles and residences with adequate security features

You can greatly increase your personal protection posture by remaining anonymous and reducing your exposure.

Select Next to continue.

A Motivational Use Case Example

- Safe back in her room at the Repressia Grand Hotel, PO Alice wants to read and/or post to sealiftcommand.com



Civilian Maritime Jobs | MSC | Military Sealift Command
Without Computer Security, Sou...
Civilian Maritime Jobs | MSC | M...
https://www.sealiftcommand.com
Google

MILITARY SEALIFT COMMAND

MSC
Like 4k
ABOUT MSC
MARITIME EMPLOYMENT RESOURCES
START THE PROCESS
CONTACT US

A plugin is required to play additional media on this page.
Please download Adobe Flash Player.

NEWS AND ANNOUNCEMENTS

Military Sealift Command Accepts Navy's Newest Ship, USNS William McLean

SAN DIEGO (NNS) — Military Sealift Command accepted delivery of dry cargo/ammunition ship USNS William McLean (T-AKE 12) during a ceremony at the General Dynamics NASSCO shipyard in San Diego Sept. 28. The 689-foot long McLean, designated T-AKE 12, is the 12th of 14 new Read More →

LET'S TALK JOBS

Career Fairs RSS. View all career fairs→

11.03.11	**MSC Career Fair** San Francisco, CA | 9:30AM - 1:30PM
11.03.11	**MSC Career Fair – MILITARY ONLY** Millington, TN | 11AM - 3PM
11.03.11	**MSC Career Fair** Pensacola, FL | 11AM - 3PM
11.09.11	**Hire a Vet Career Fair** Raleigh, NC | 10AM - 3PM
11.10.11	**Recruit Military Veterans Expo** Miami, FL | 11AM - 3PM

NOW HIRING

Now Hiring RSS. View all open positions→

Able Seaman
Announcement open 1 November through 30 November 2011.

Medical Services Officer
Announcement open 3 October 2011, with periodic cut-offs.

Second Cook
Announcement open 5 October 2011, with periodic cut-offs.

GETTING STARTED

Resources to help you take command of your career.

Your previous experience can make a difference in a maritime career with MSC

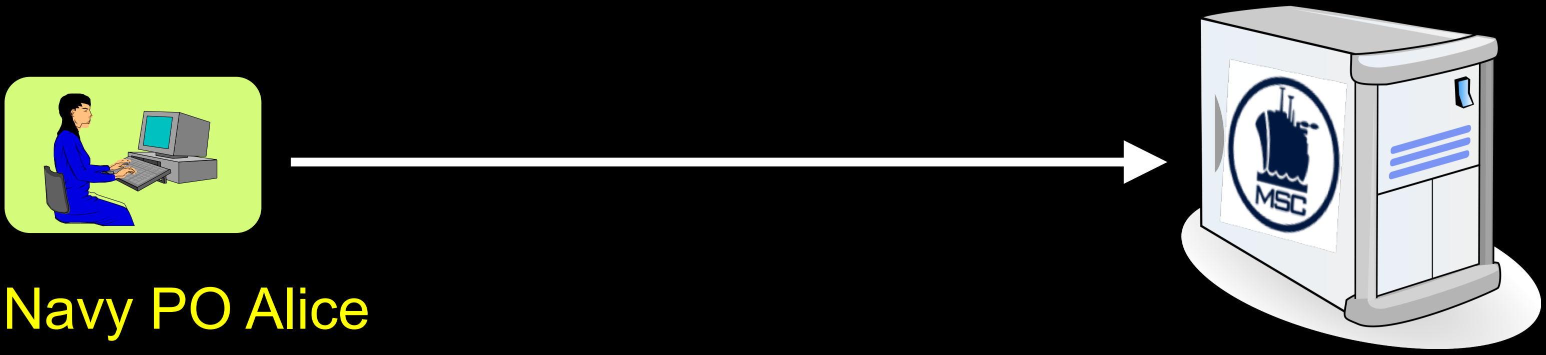
- Current Mariners
- Departing Military
- Maritime School Graduates
- Entry Level/Skilled Laborers

Take Command of Your Career®

Home U.S. Navy U.S. Coast Guard Military Sealift Fleet Support Command Contact Us Privacy Policy

MSC is an Equal Opportunity Employer and Drug-Free Workplace

A Motivational Use Case Example



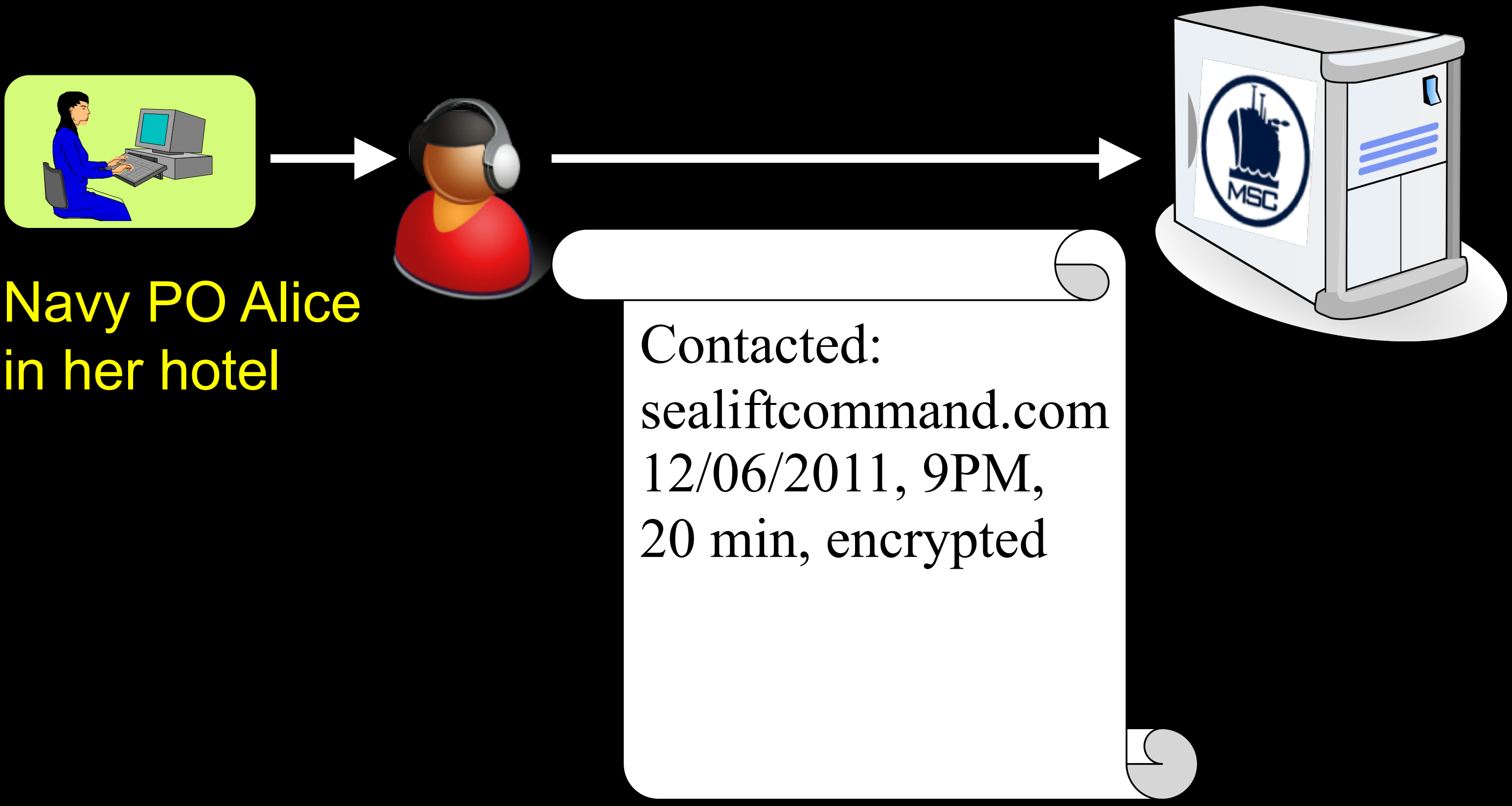
Navy PO Alice
in her hotel

A Motivational Use Case Example

- Safe back in her room at the Repressia Grand Hotel, PO Alice wants to read and/or post to sealiftcommand.com

1. The site is blocked where she is deployed
2. The Internet is monitored where she is deployed

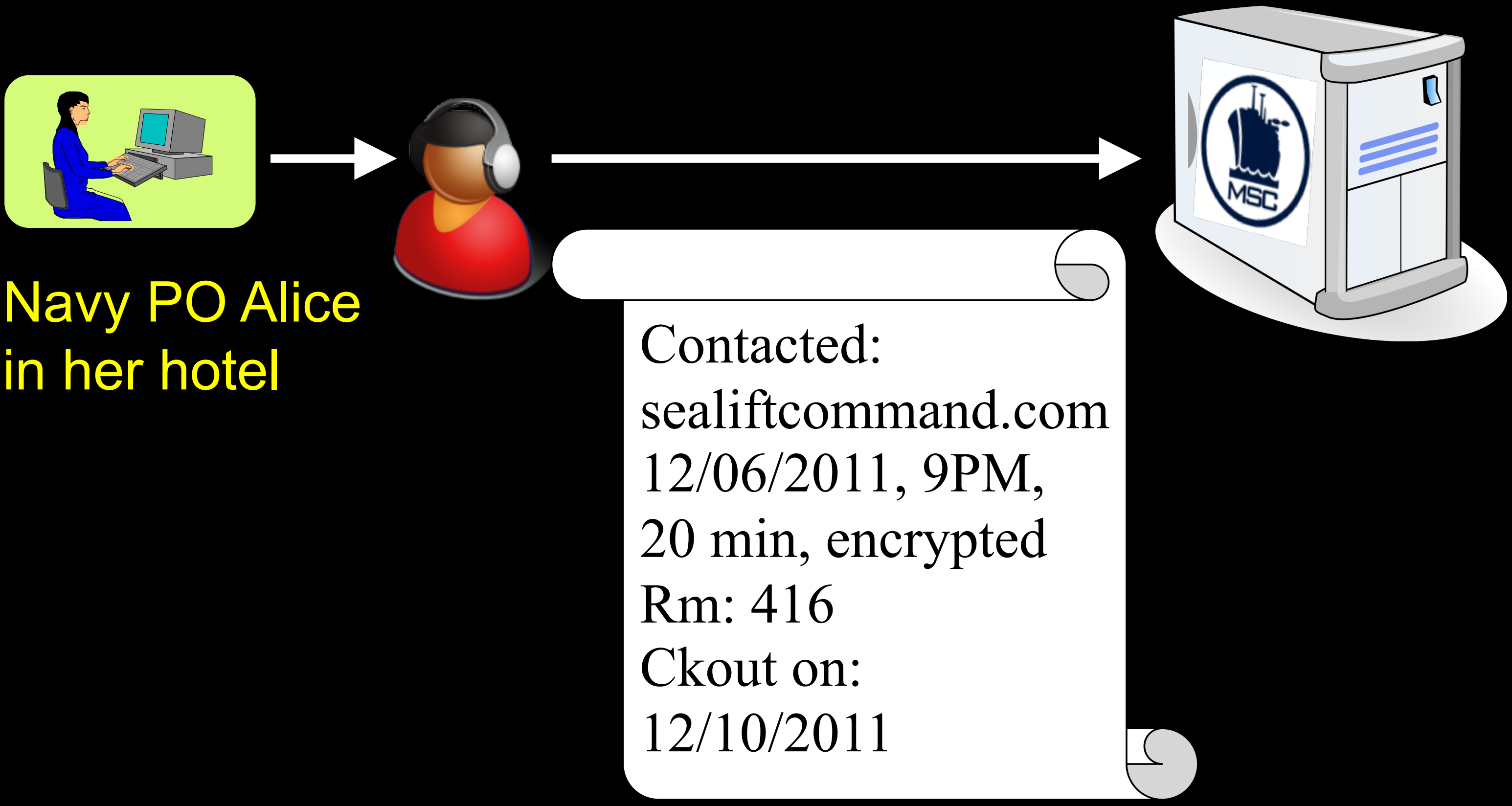
Connecting when overseas



Navy PO Alice
in her hotel

Contacted:
sealiftcommand.com
12/06/2011, 9PM,
20 min, encrypted

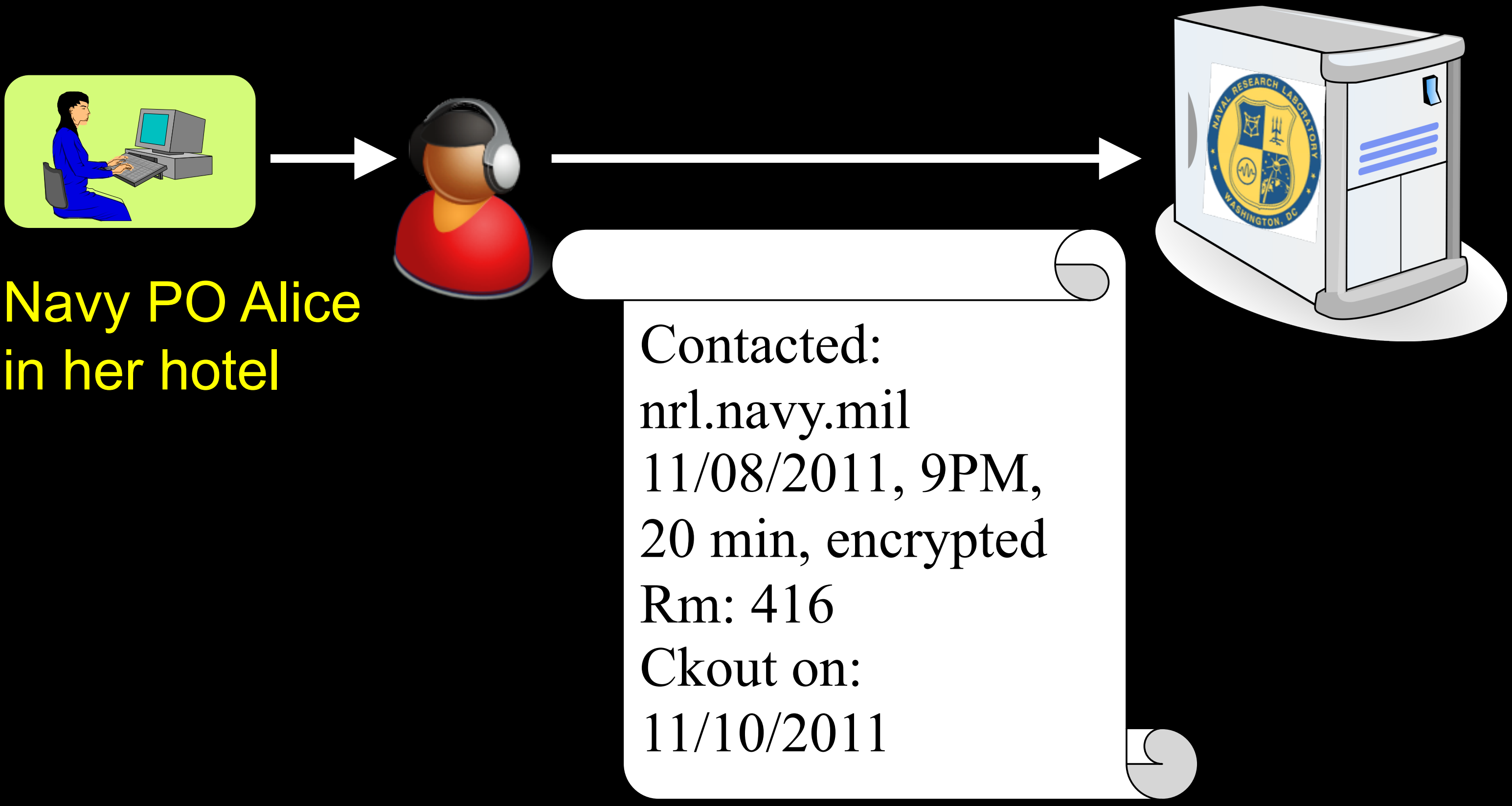
Connecting when overseas



Navy PO Alice
in her hotel

Contacted:
sealiftcommand.com
12/06/2011, 9PM,
20 min, encrypted
Rm: 416
Ckout on:
12/10/2011

Security of operations concern as well as personnel security concern



Navy PO Alice
in her hotel

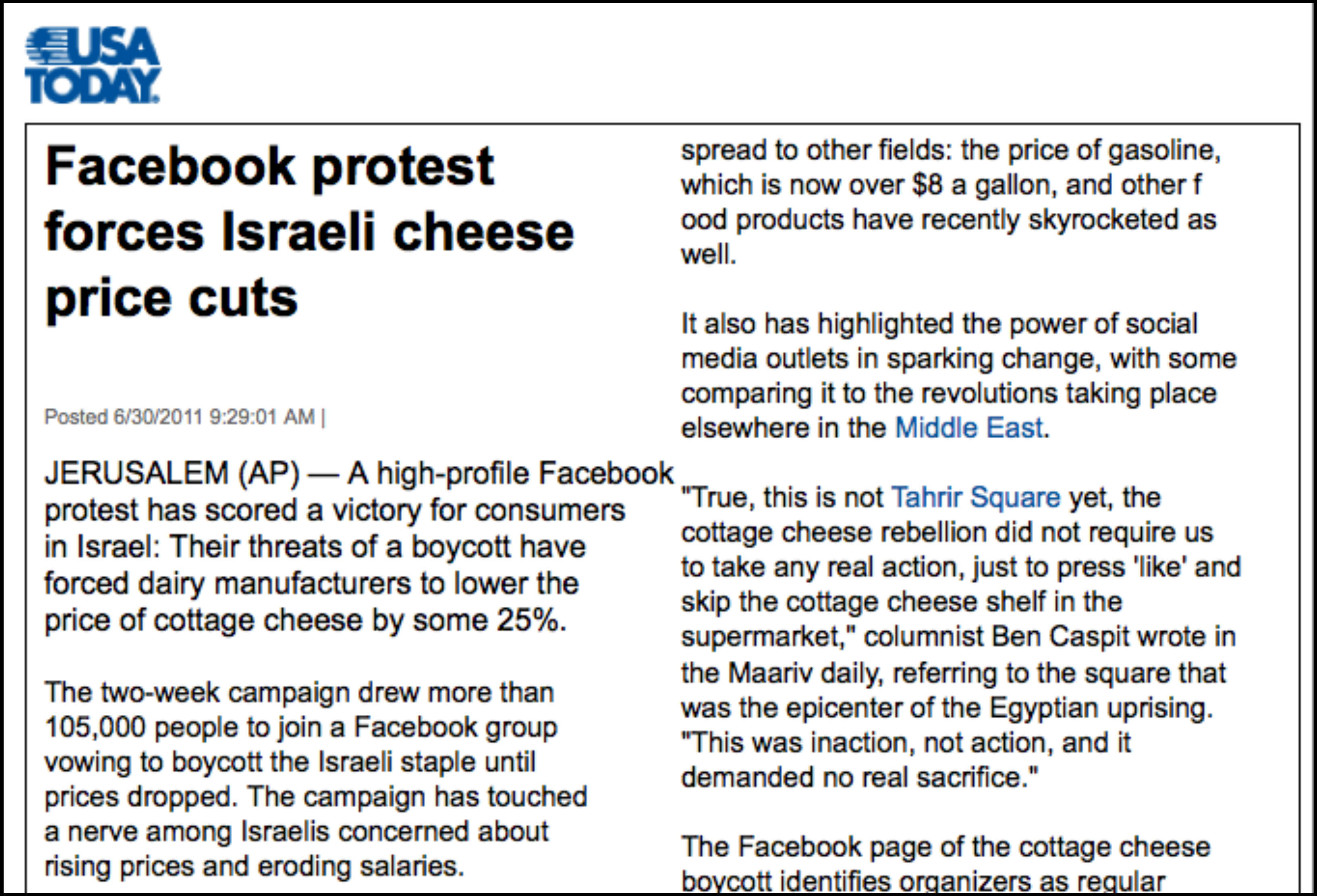
Contacted:
nrl.navy.mil
11/08/2011, 9PM,
20 min, encrypted
Rm: 416
Ckout on:
11/10/2011

Some more government uses

- Open source intelligence gathering
- Sensitive communications with untrusted/ untrusting parties
- Encouraging open communications with citizens
- Location protected servers for defense in depth
- Protecting the public infrastructure
  - Interacting with network sensors

Ordinary citizen Alice

- Protecting her behavior from:
- Cyberstalking abusive ex-spouse
- Behavior tracking and DNS shenanigans from her ISP
- Misunderstanding from her employer when she investigates disease info for an ailing friend
- Harassment for blogging her views



USA TODAY

Facebook protest forces Israeli cheese price cuts

Posted 6/30/2011 9:29:01 AM |

JERUSALEM (AP) — A high-profile Facebook protest has scored a victory for consumers in Israel: Their threats of a boycott have forced dairy manufacturers to lower the price of cottage cheese by some 25%.

The two-week campaign drew more than 105,000 people to join a Facebook group vowing to boycott the Israeli staple until prices dropped. The campaign has touched a nerve among Israelis concerned about rising prices and eroding salaries.

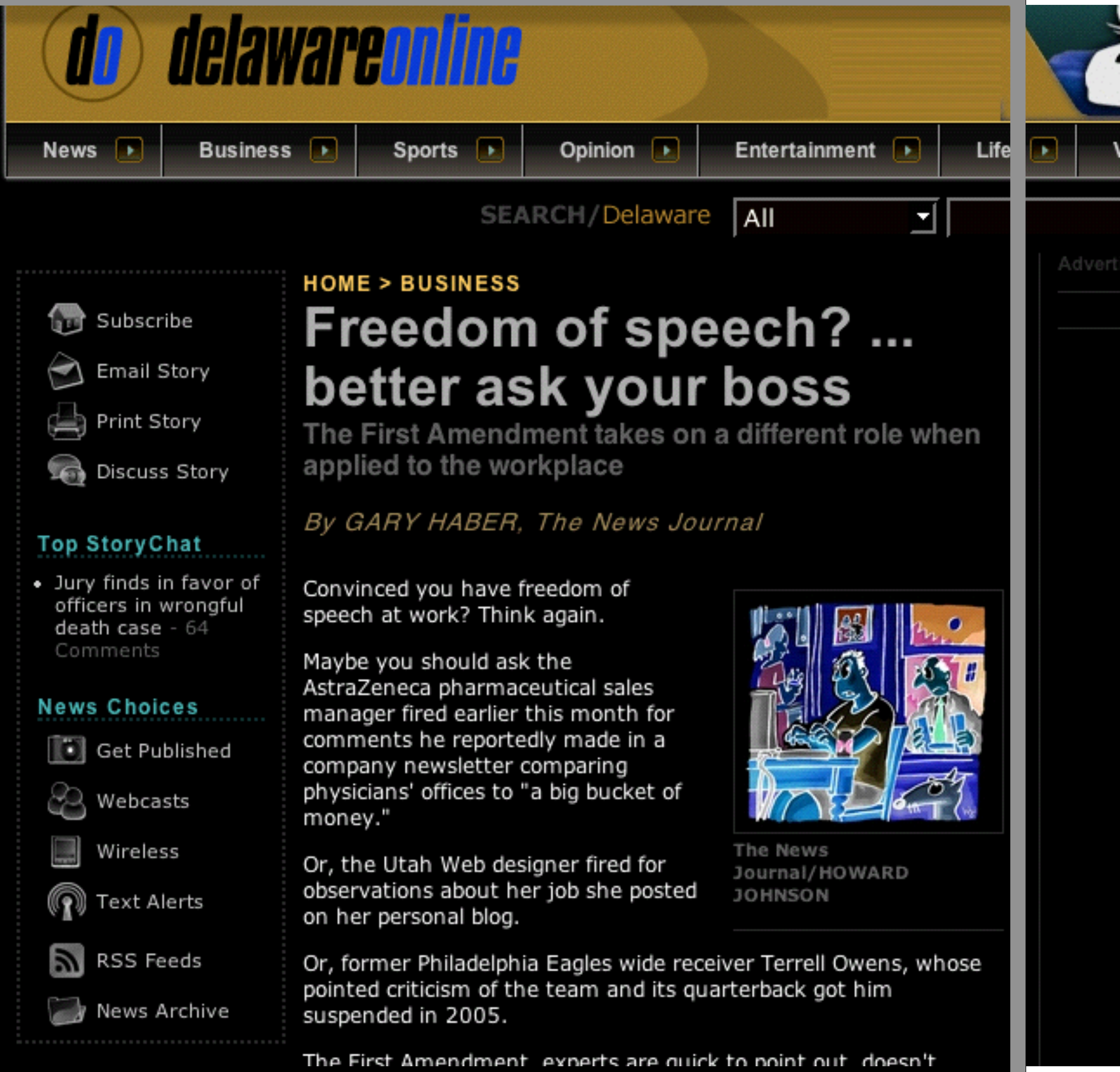
spread to other fields: the price of gasoline, which is now over $8 a gallon, and other f ood products have recently skyrocketed as well.

It also has highlighted the power of social media outlets in sparking change, with some comparing it to the revolutions taking place elsewhere in the Middle East.

"True, this is not Tahrir Square yet, the cottage cheese rebellion did not require us to take any real action, just to press 'like' and skip the cottage cheese shelf in the supermarket," columnist Ben Caspit wrote in the Maariv daily, referring to the square that was the epicenter of the Egyptian uprising. "This was inaction, not action, and it demanded no real sacrifice."

The Facebook page of the cottage cheese boycott identifies organizers as regular

It's not only about dissidents in faraway lands



- Jury finds in favor of officers in wrongful death case - 64 Comments

HOME > BUSINESS

Freedom of speech? ... better ask your boss

The First Amendment takes on a different role when applied to the workplace

By GARY HABER, The News Journal

Convinced you have freedom of speech at work? Think again.

Maybe you should ask the AstraZeneca pharmaceutical sales manager fired earlier this month for comments he reportedly made in a company newsletter comparing physicians' offices to "a big bucket of money."

Or, the Utah Web designer fired for observations about her job she posted on her personal blog.

The News Journal/HOWARD JOHNSON

Or, former Philadelphia Eagles wide receiver Terrell Owens, whose pointed criticism of the team and its quarterback got him suspended in 2005.

The First Amendment, experts are quick to point out, doesn't

Ordinary citizen Alice

- Protecting her behavior from:
- Cyberstalking abusive ex-spouse
- Behavior tracking and DNS shenanigans from her ISP
- Misunderstanding from her employer when she investigates disease info for an ailing friend
- Harassment for blogging her views

Ordinary citizen Alice

- Protecting her behavior from:
- Cyberstalking abusive ex-spouse
- Behavior tracking and DNS shenanigans from her ISP
- Misunderstanding from her employer when she investigates disease info for an ailing friend
- Harassment for blogging her views
- Malicious parties watching her log into Club Penguin (and watching her mom logged into twitter from work)
- Spear phishers watching her log into her bank

Officer Alice

- Setting up a sting operation:
  - as a collaborator
  - as a service provider
- Monitoring criminal activity online
- Encouraging anonymous tips

Researcher/Reporter/Rights Worker Alice

- Gathering information while protecting sources
- Accessing information that is locally censored or monitored
- Reporting information that is locally censored or monitored

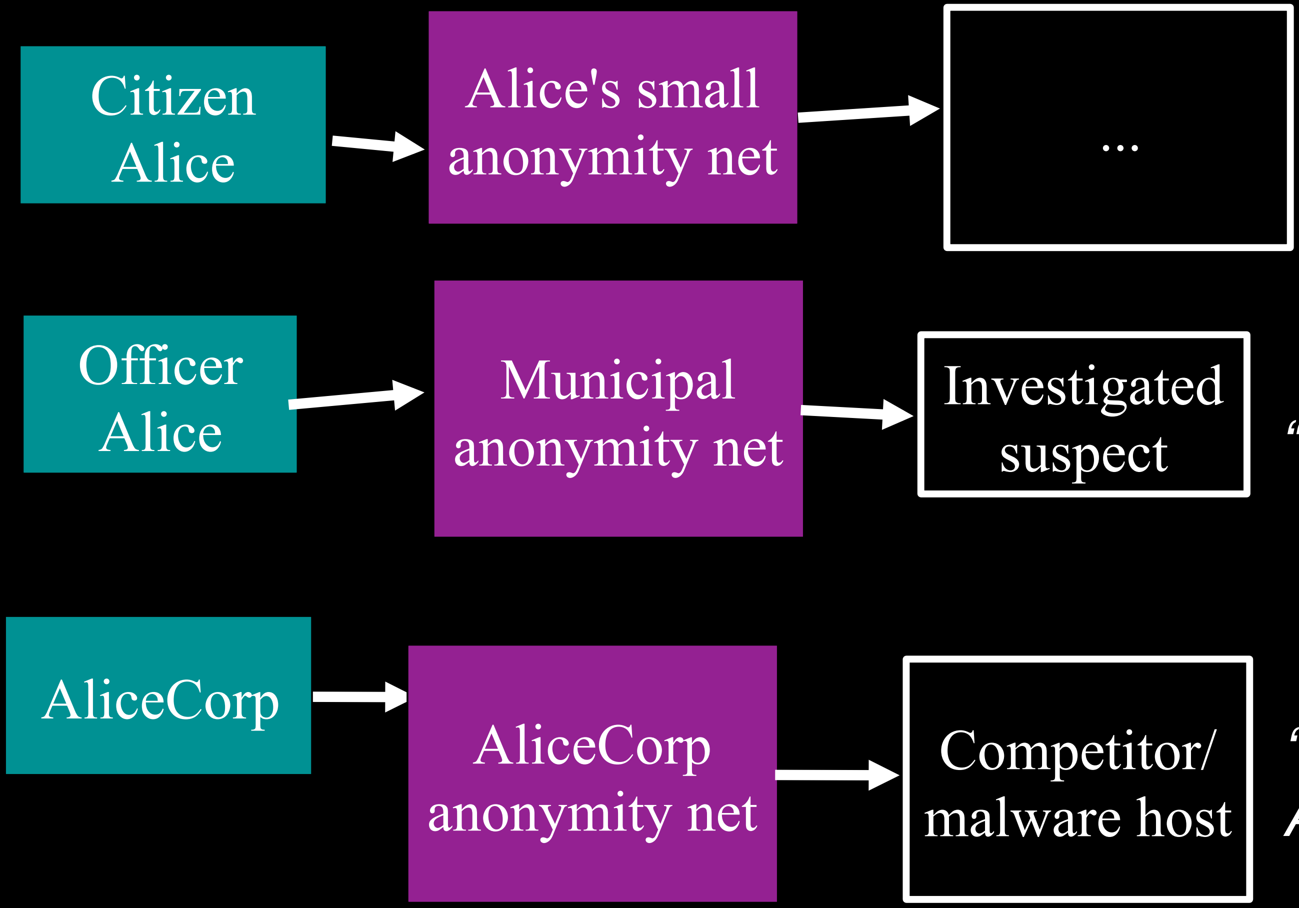
Corporation Alice

- Investigating competitors’ public sites
- Avoiding leaking strategy or nonpublic information
- Protecting customers
  - spearphishing
  - attacks or selective service disruption
  - privacy sensitivity

Aside: some other benefits of an anonymity system

- Besides protecting affiliation, etc. can provide “poor man’s VPN”. Access to the internet despite
  - Network port policy disconnects
  - DNS failure

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



Citizen Alice

Alice's small anonymity net

...

"One of the 25 users on AliceNet."

Officer Alice

Municipal anonymity net

Investigated suspect

"Looks like a cop."

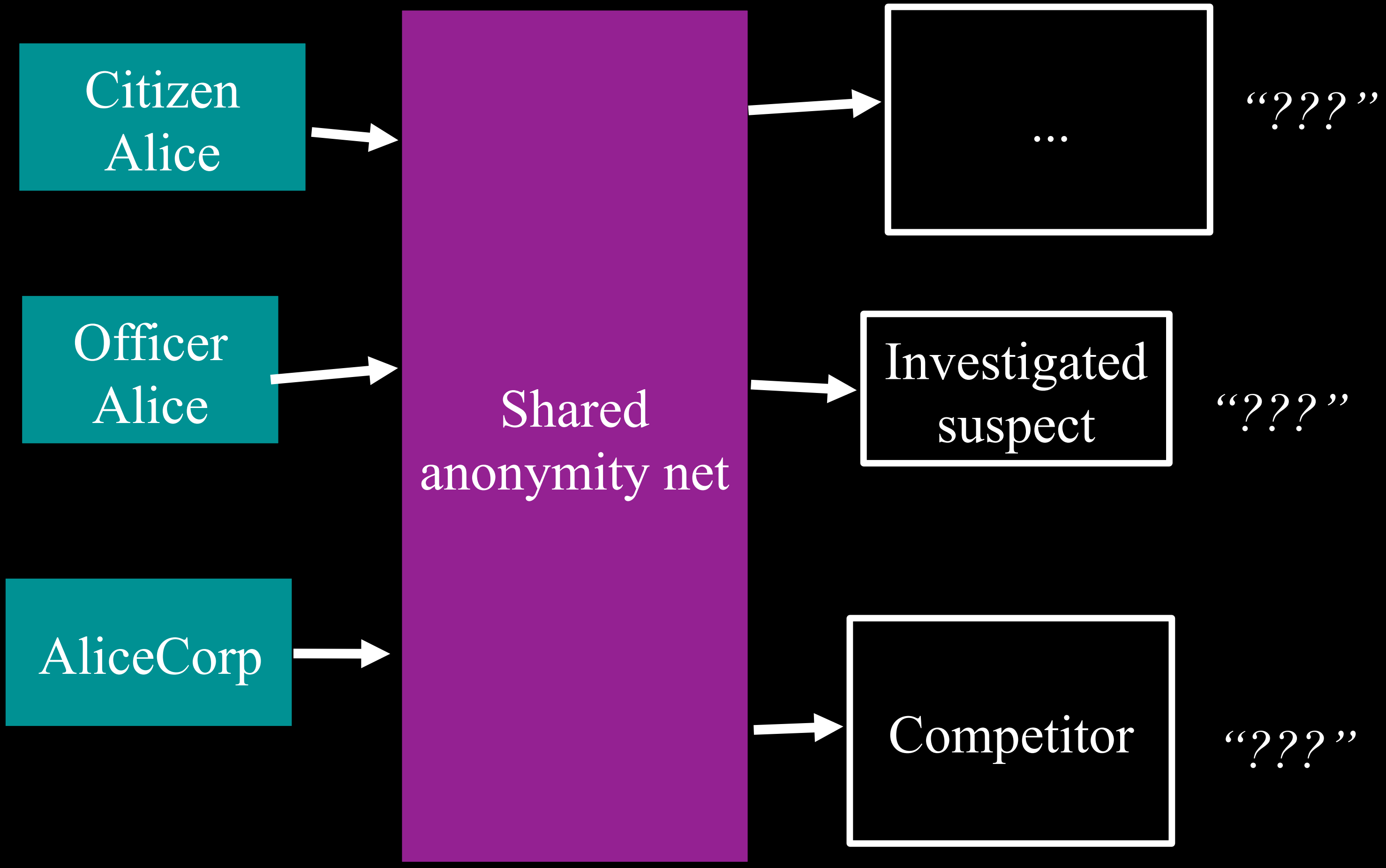
AliceCorp

AliceCorp anonymity net

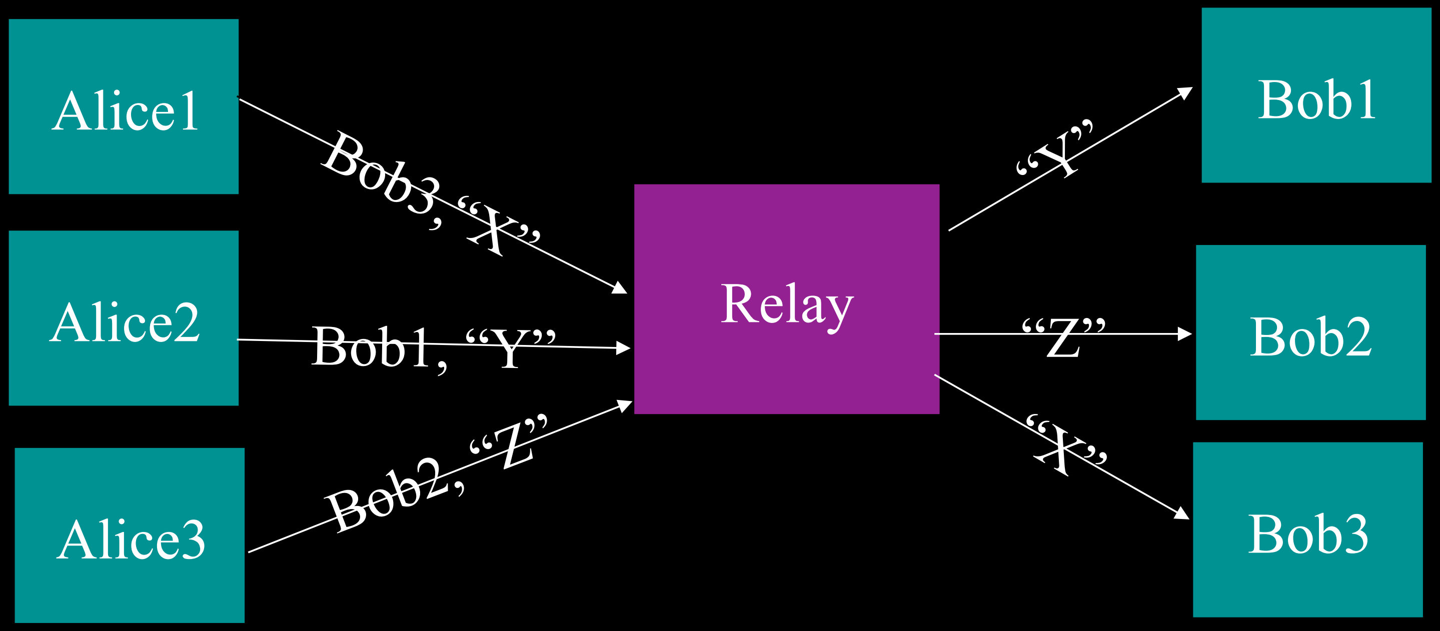
Competitor/ malware host

*"It's **somebody** at AliceCorp!"*

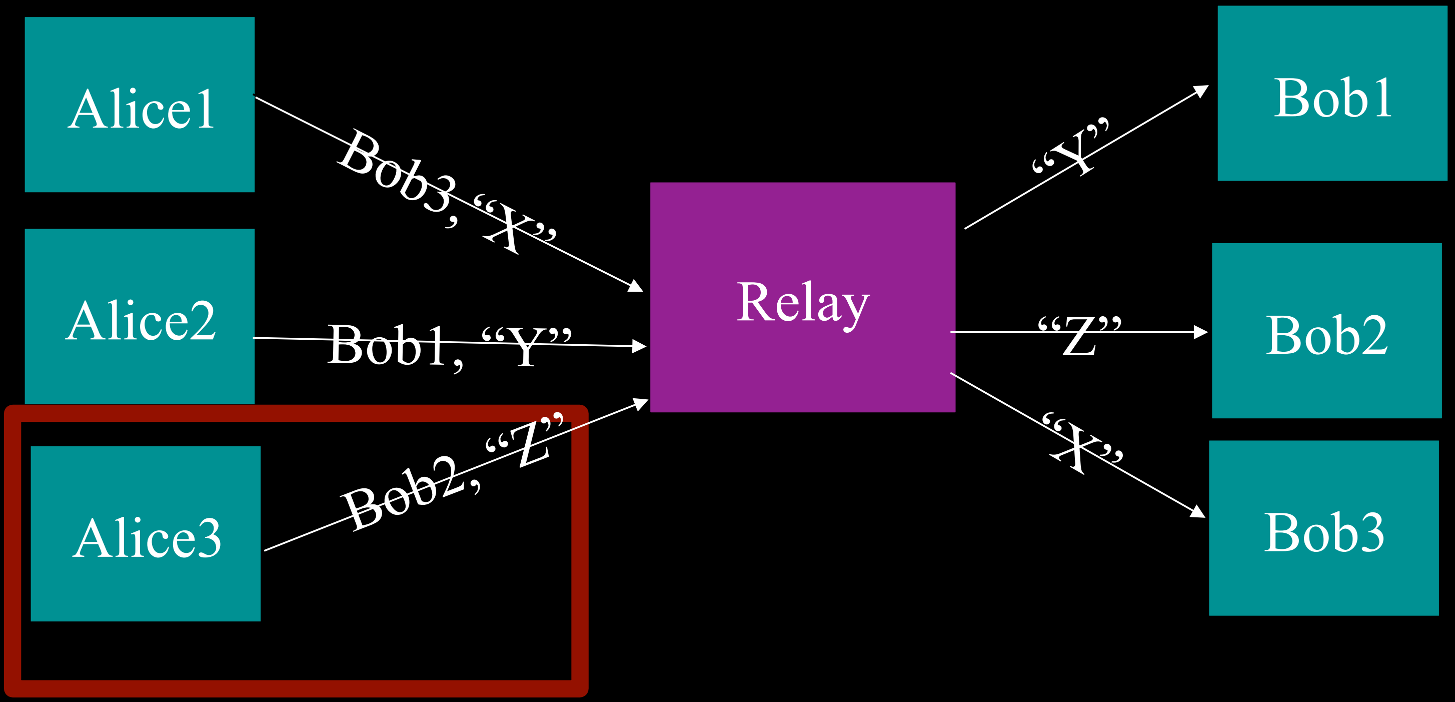
... so, anonymity loves company!



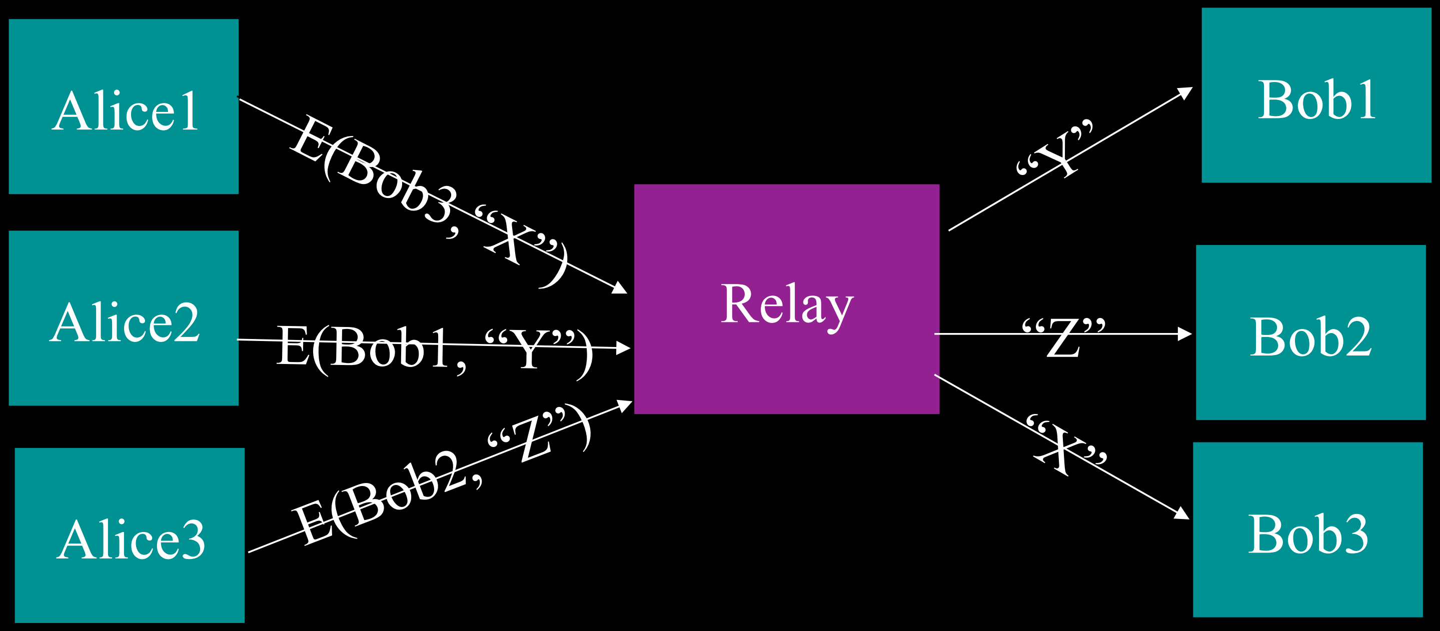
The simplest designs use a single relay to hide connections.



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

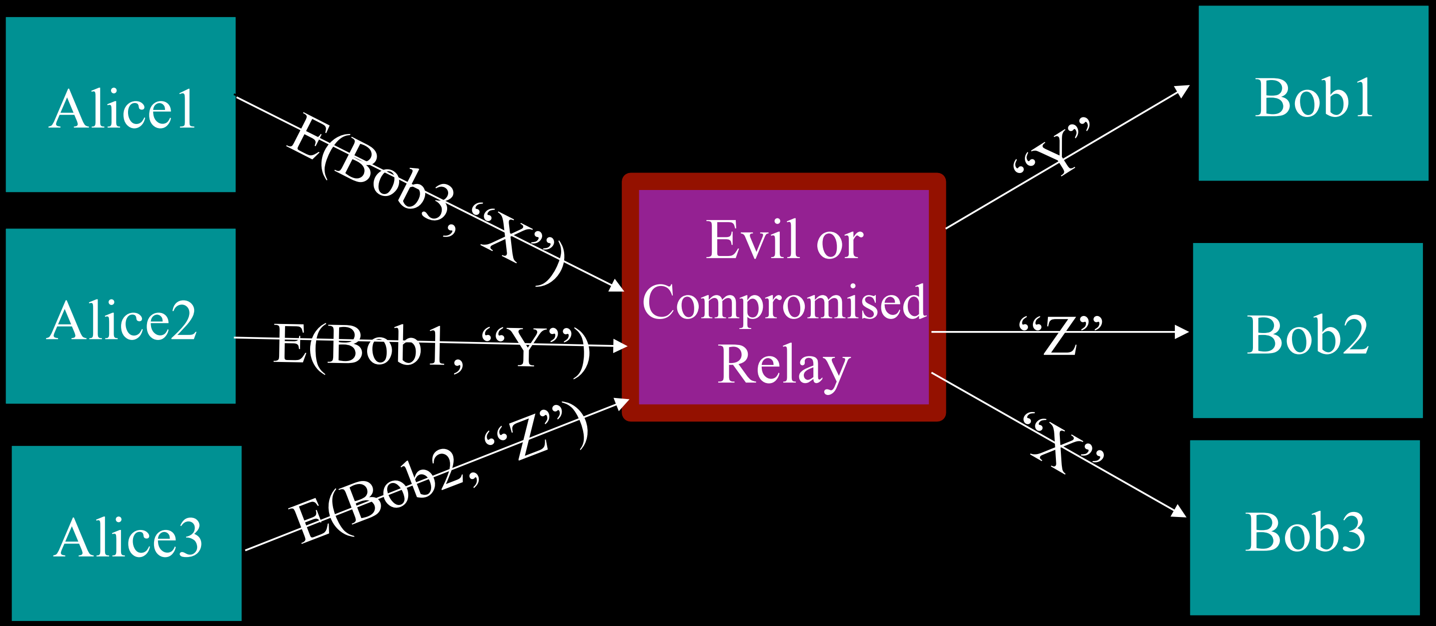


Add encryption to stop attackers who eavesdrop on Alice.

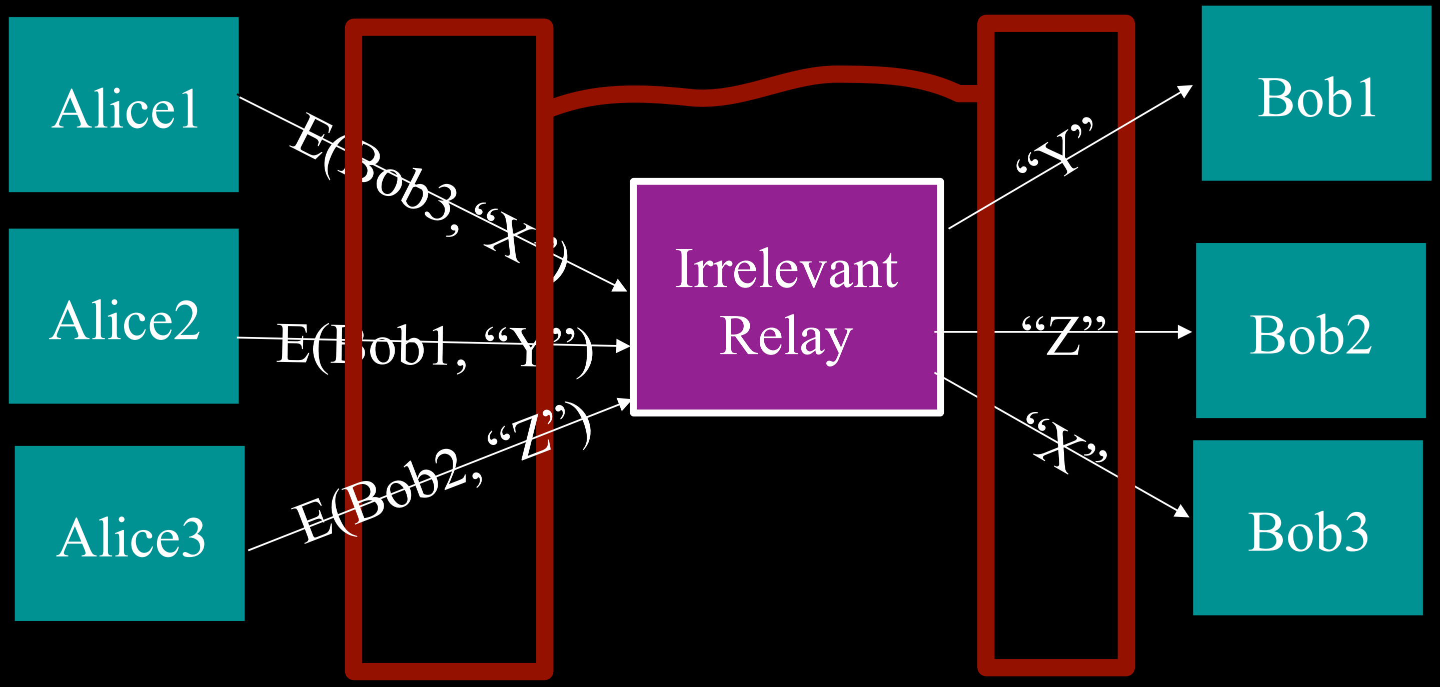


(e.g.: some commercial proxy providers, Anonymizer)

But a single relay is a single point of failure.

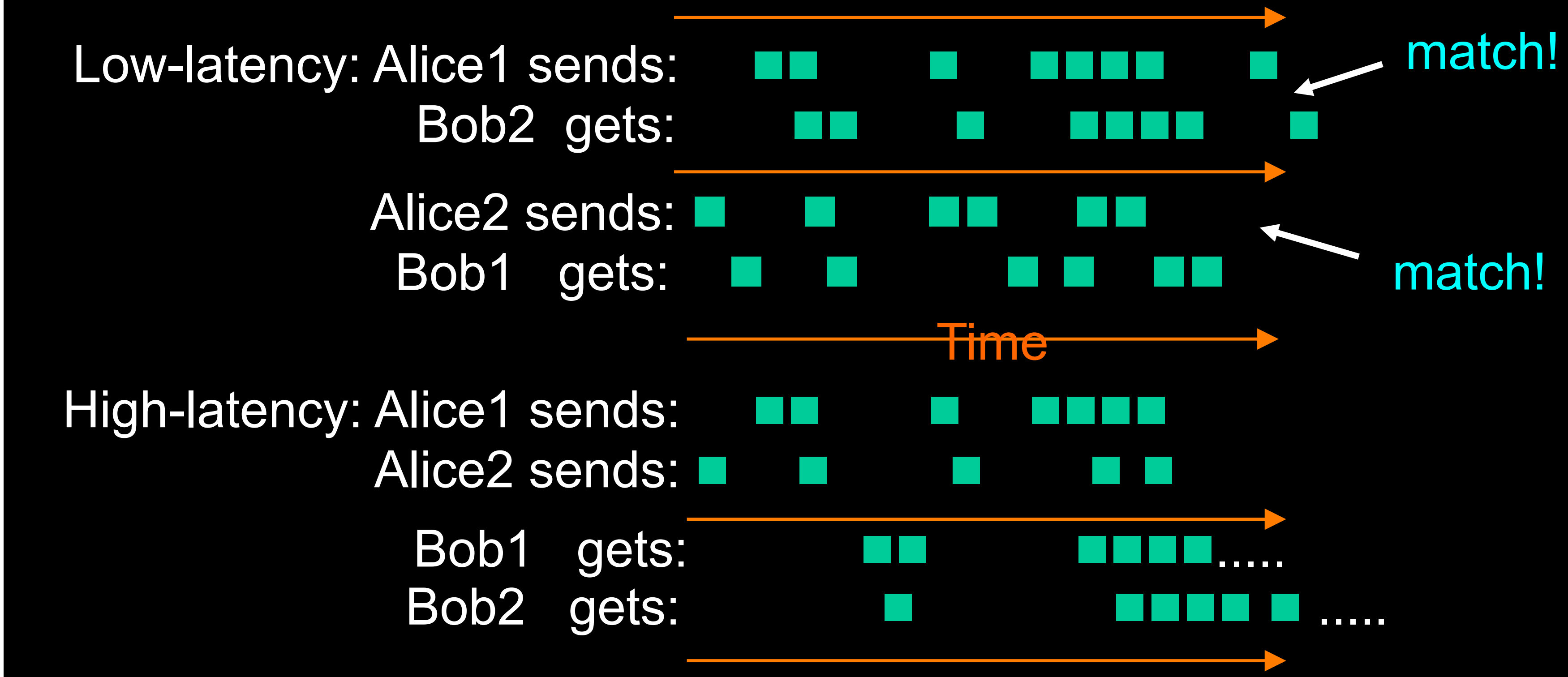


But a single relay is a single point of bypass.



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

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



Low-latency: Alice1 sends:

Bob2 gets:

Alice2 sends:

Bob1 gets:

match!

match!

Time

High-latency: Alice1 sends:

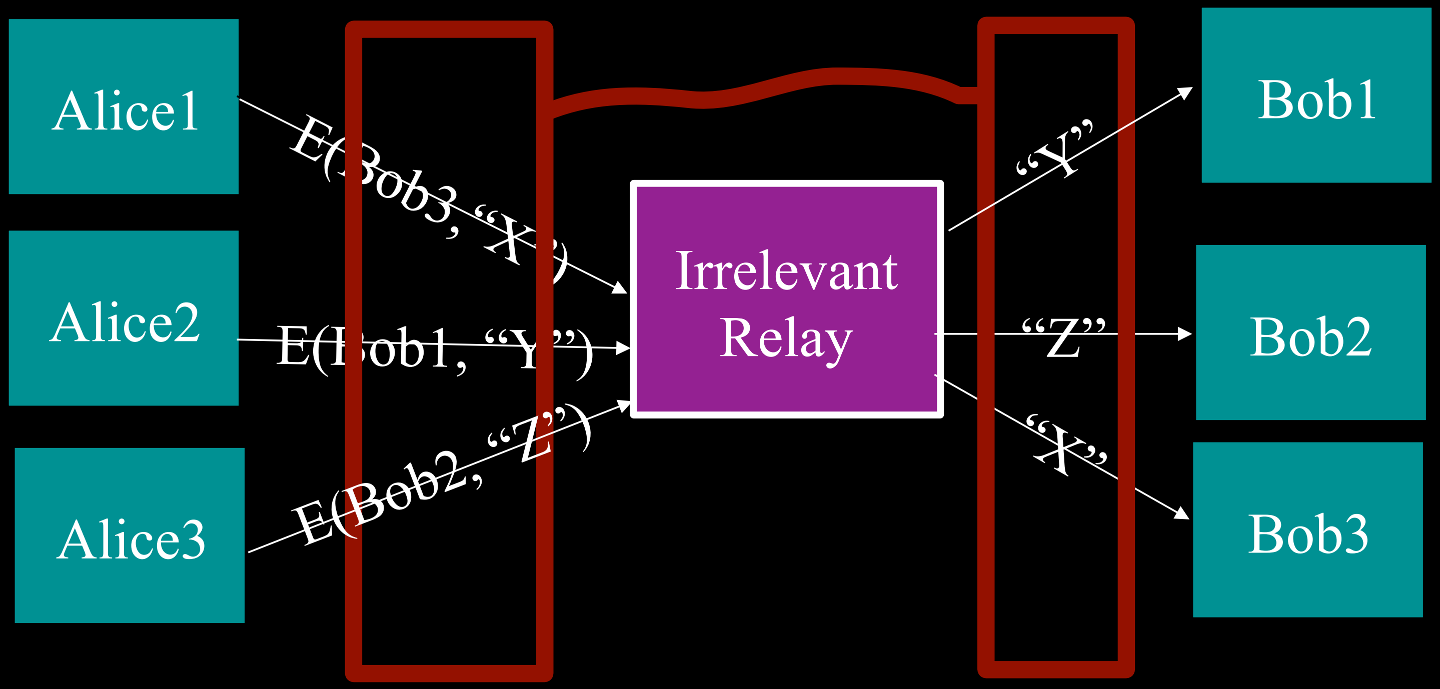
Alice2 sends:

Bob1 gets: .....

Bob2 gets: .....

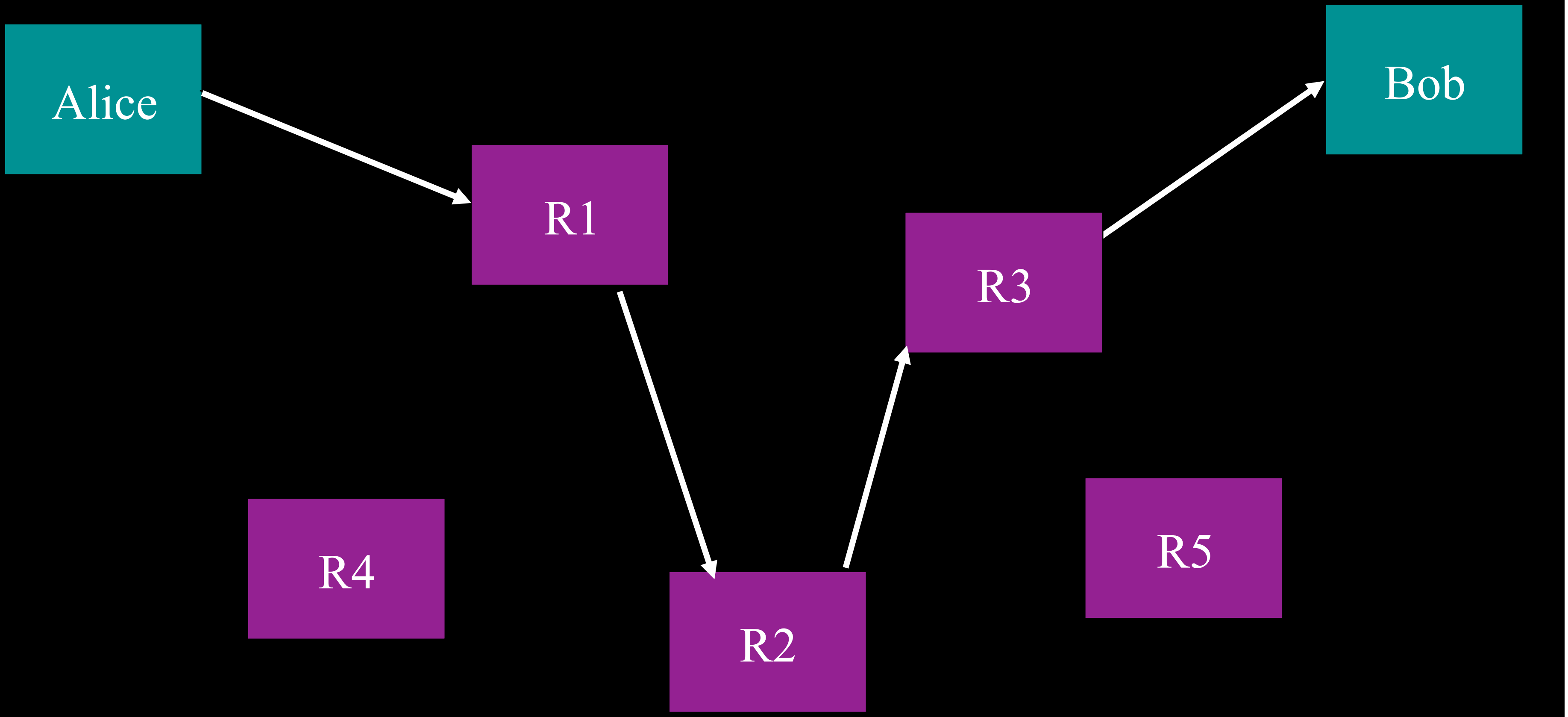
These attacks work in practice. The obvious defenses are expensive (like high-latency), useless, or both.

But a single relay is a single point of bypass.

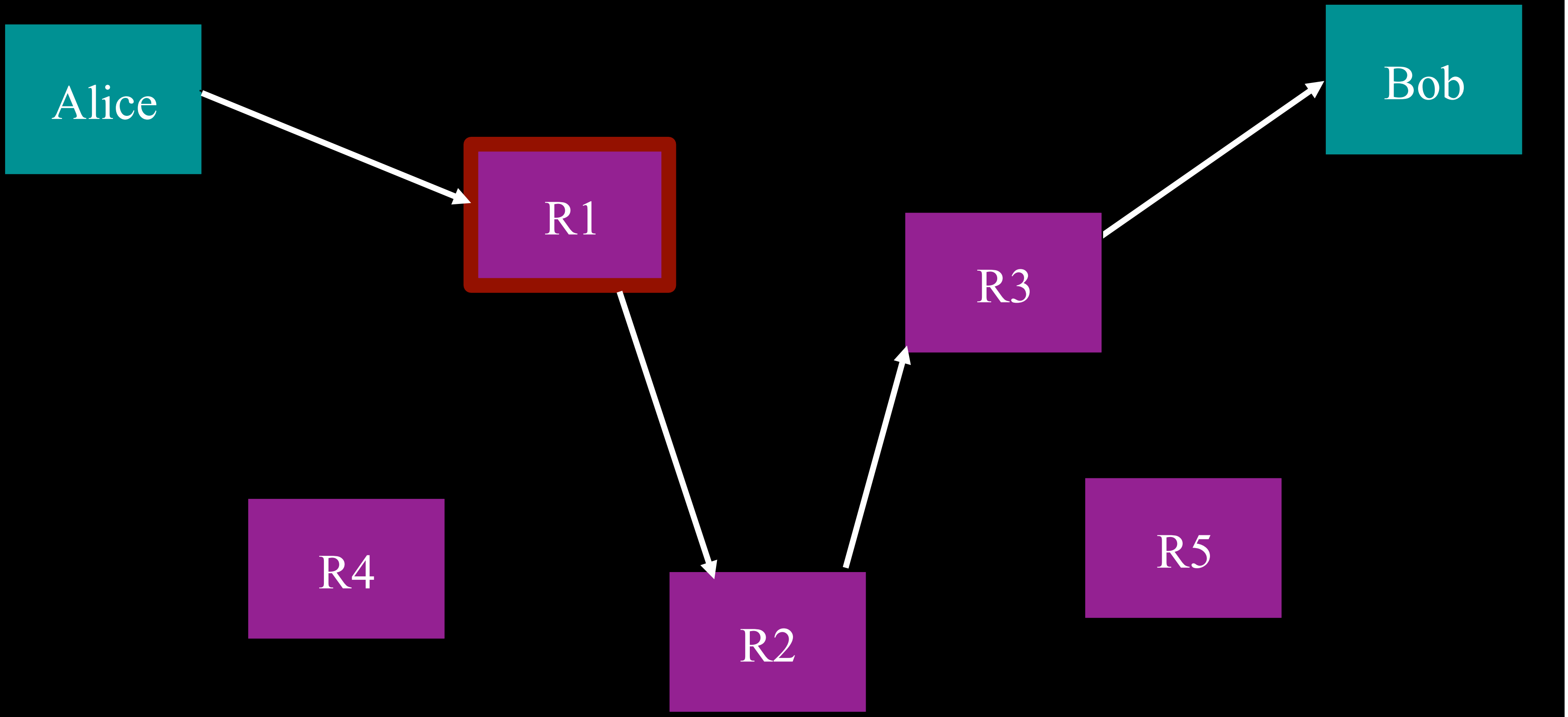


Timing analysis bridges all connections through relay ⇒ An attractive fat target

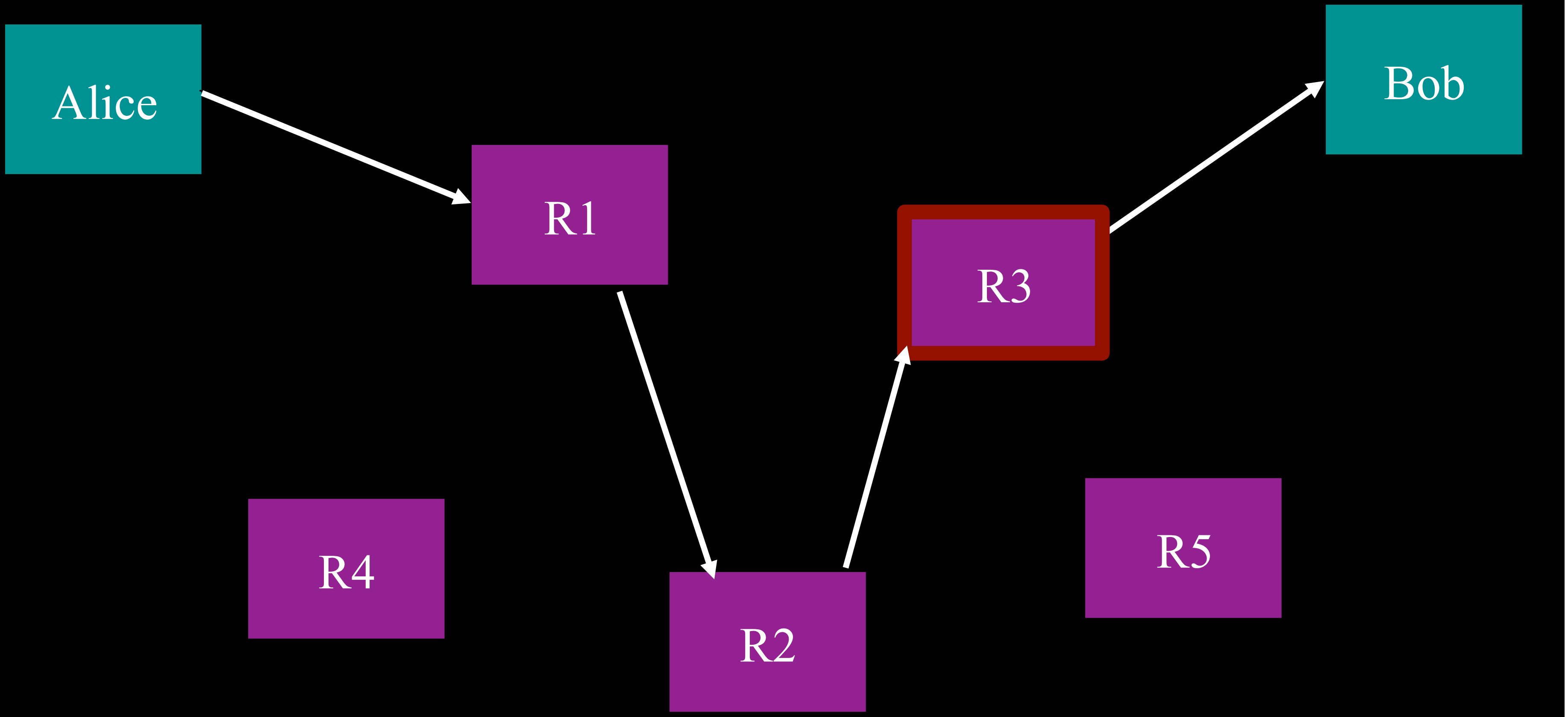
So, add multiple relays so that no single one can betray Alice.



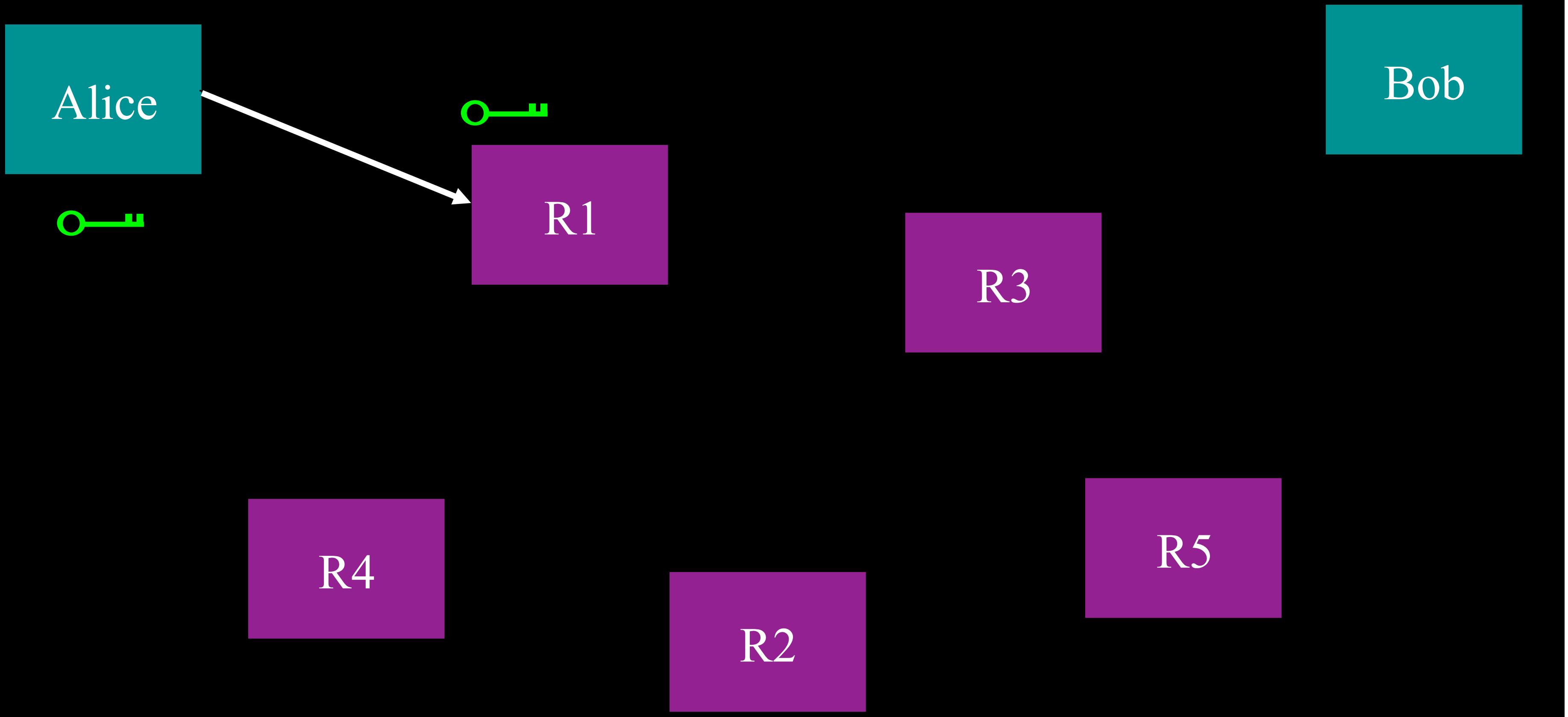
A corrupt first hop can tell that Alice is talking, but not to whom.



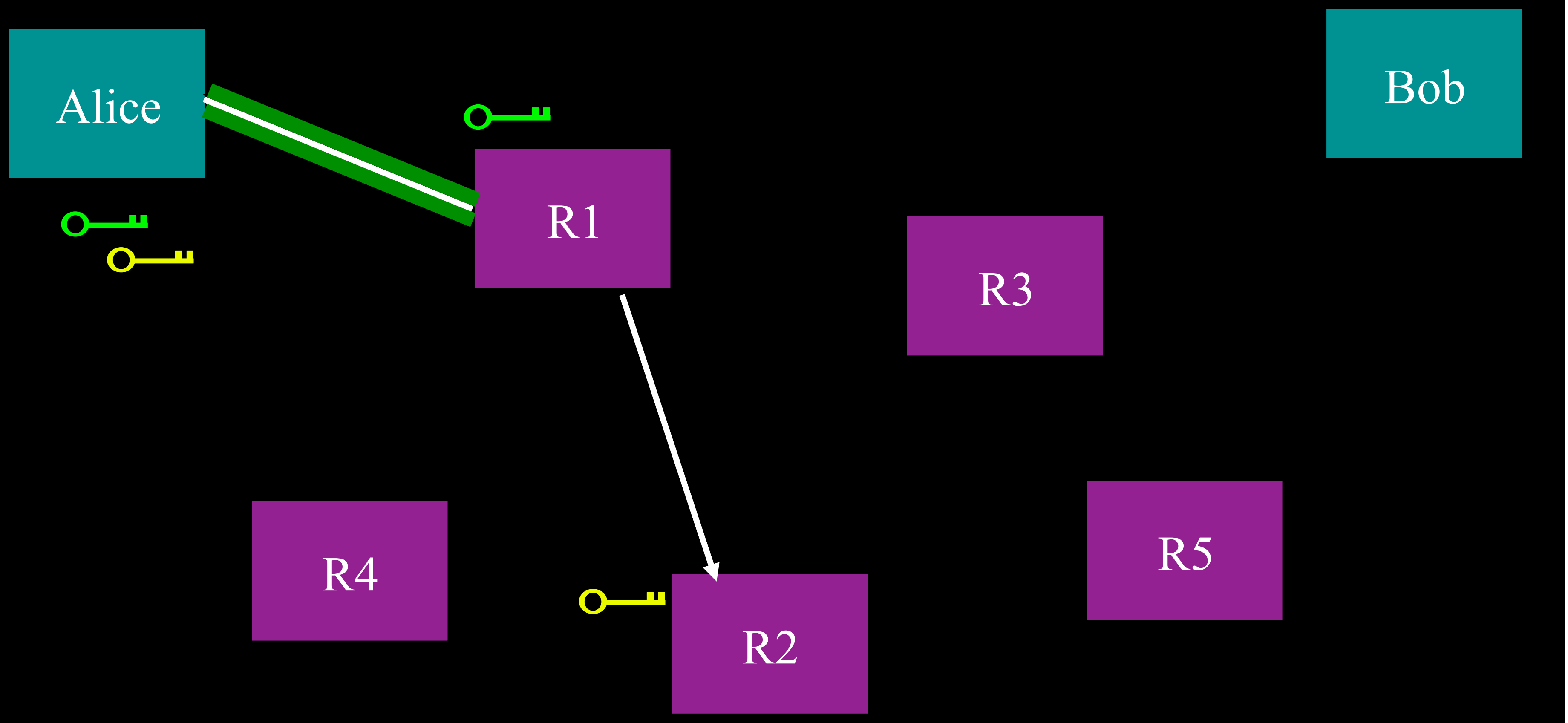
A corrupt last hop can tell someone is talking to Bob, but not who.



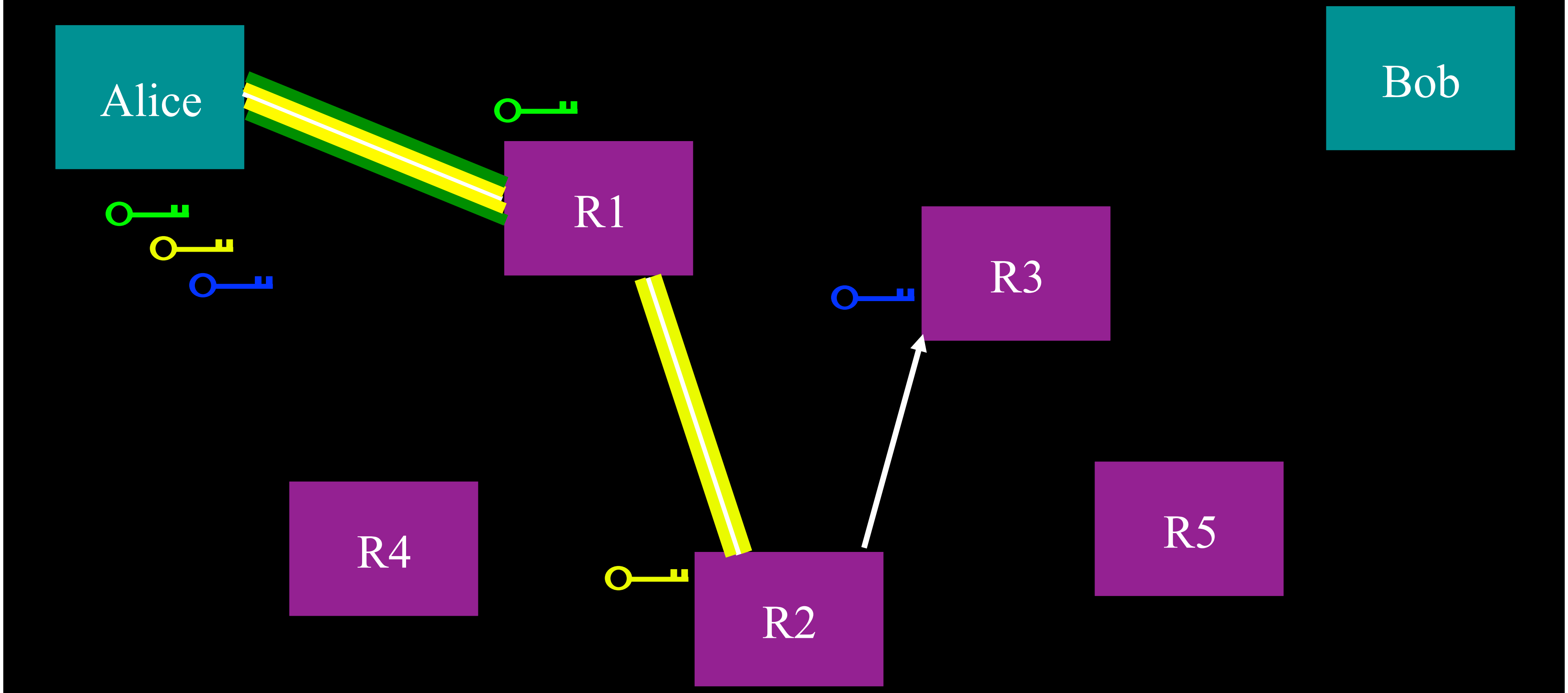
How onion routing works: Alice makes a session key with R1



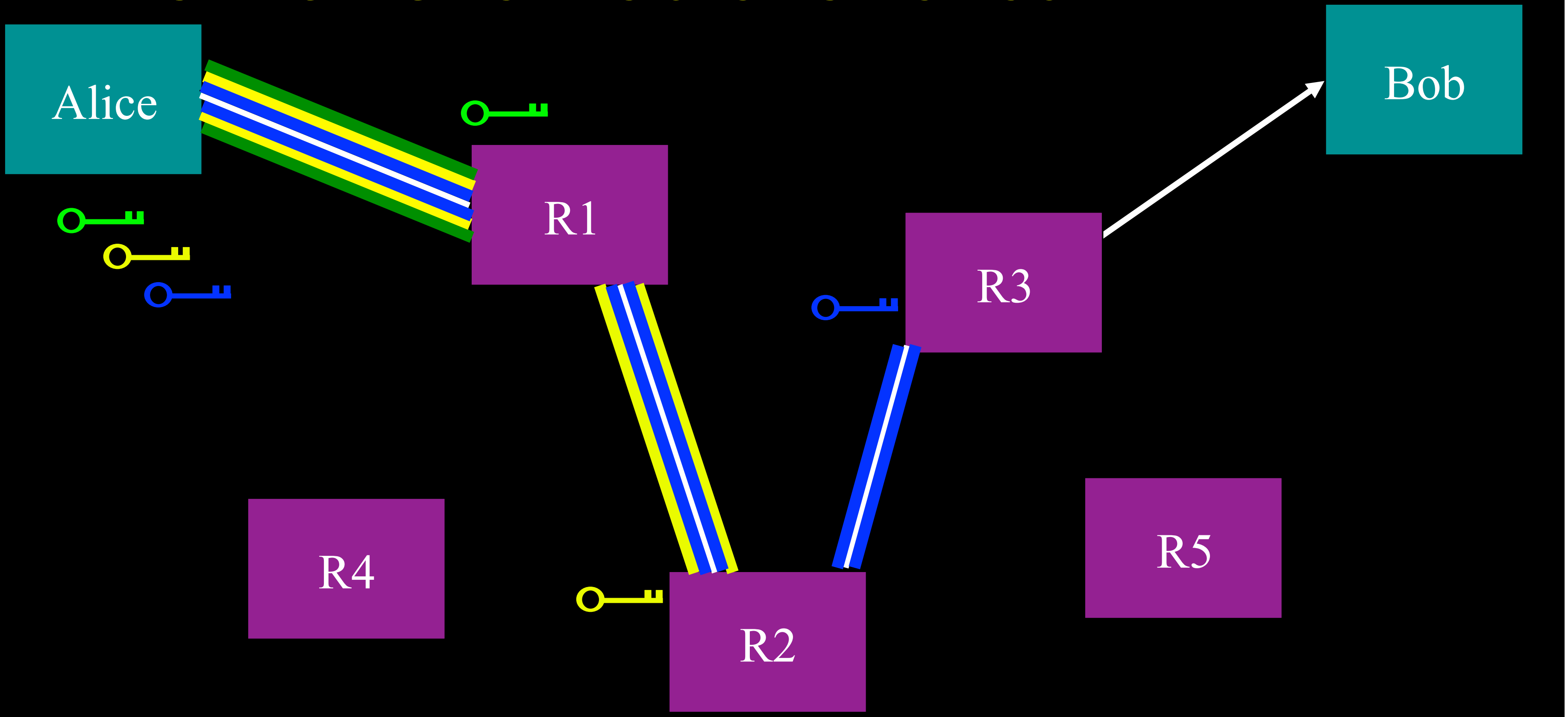
Alice makes a session key with R1
...And then tunnels to R2



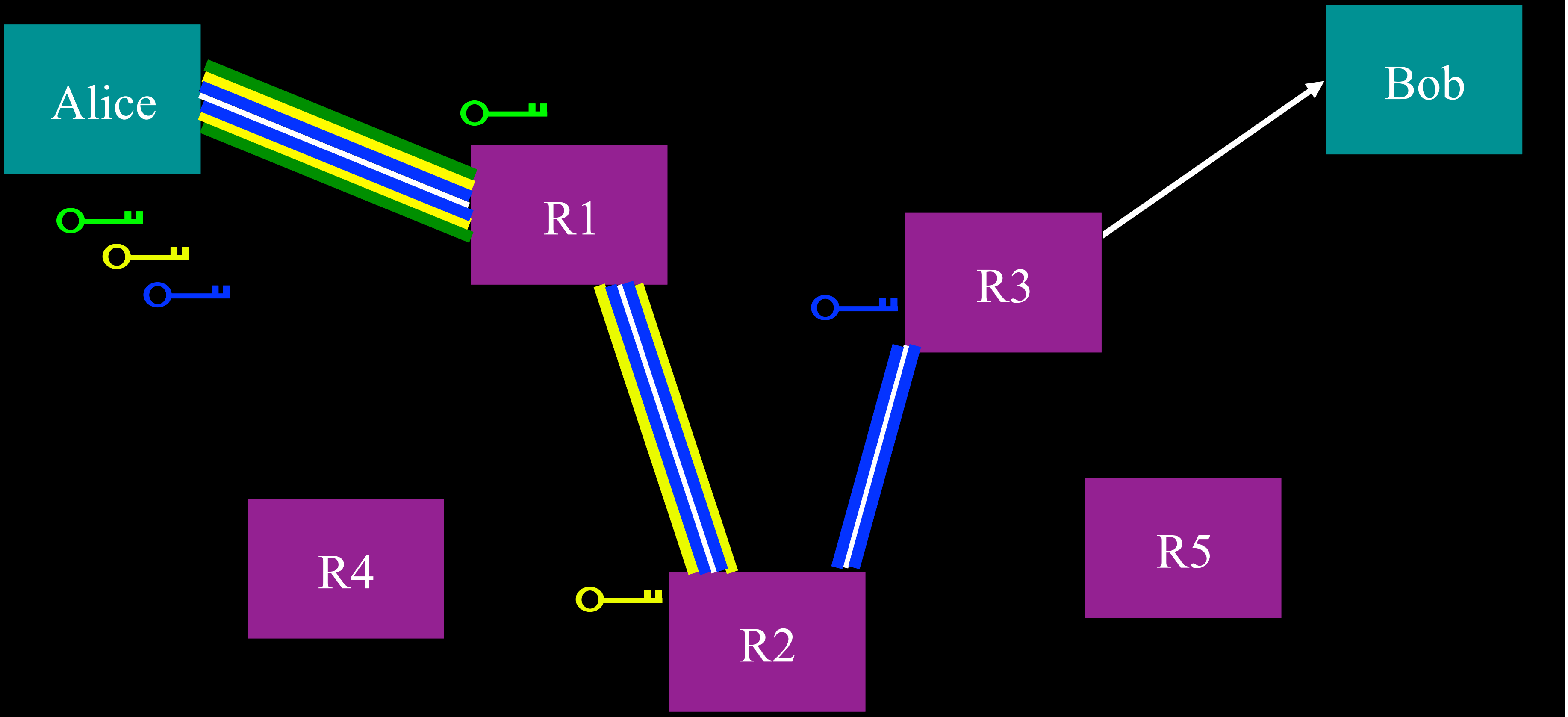
Alice makes a session key with R1 ...And then tunnels to R2...and to R3



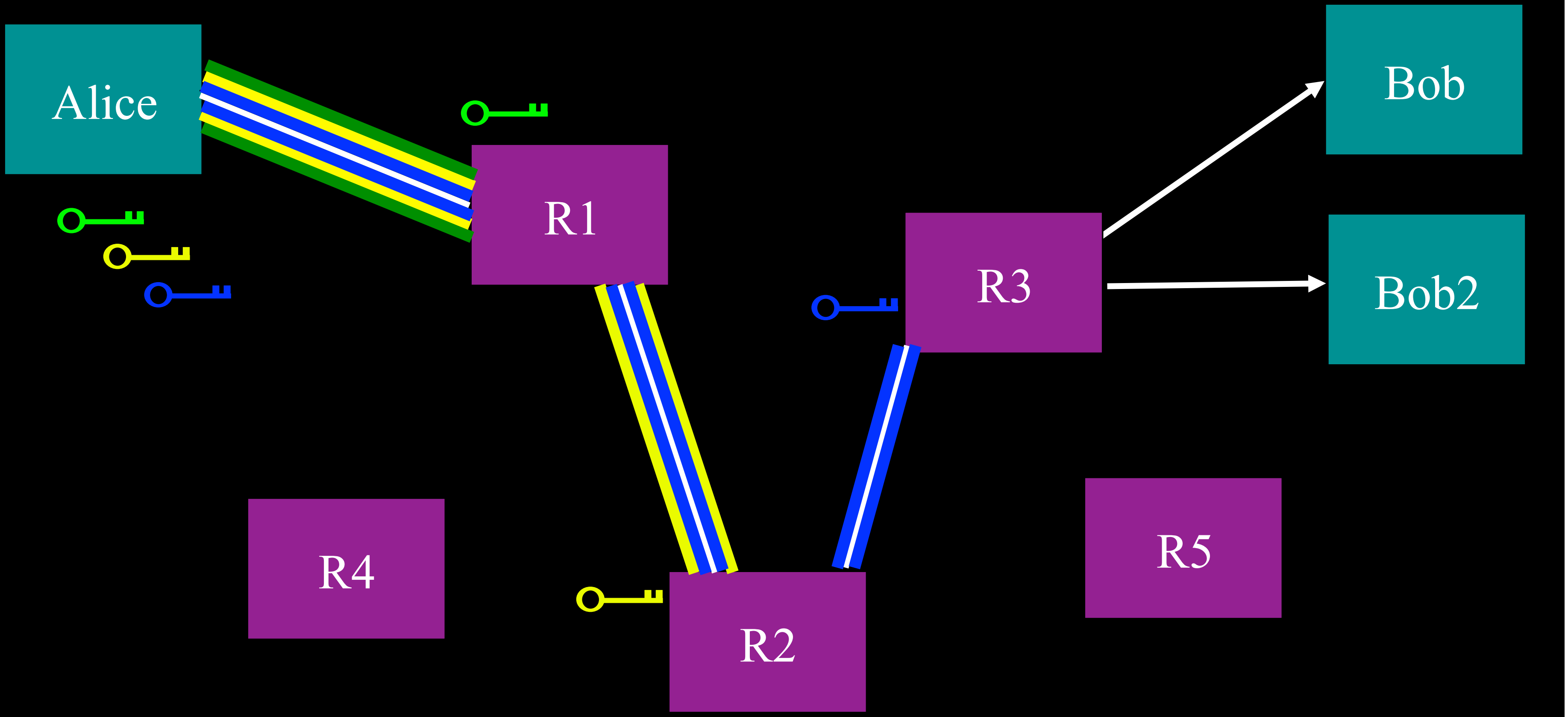
Alice makes a session key with R1 ...And then tunnels to R2...and to R3 Then talks to Bob over circuit



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 onion routing in a nutshell

What onion routing is not: Crowds

- Public-key based circuit building means
  - Forward security
  - Better practical scalability
  - Less centralized trust
- Multiply encrypted circuits means
  - less risk of route capture
  - smaller profiling threat (also from shorter circuit duration)
  - security not dependent on hiding path position
  - able to support multiple applications/application encryption options

Mix networks vs. Onion routing networks

Low-latency: Alice1 sends:

Bob2 gets:

Alice2 sends:

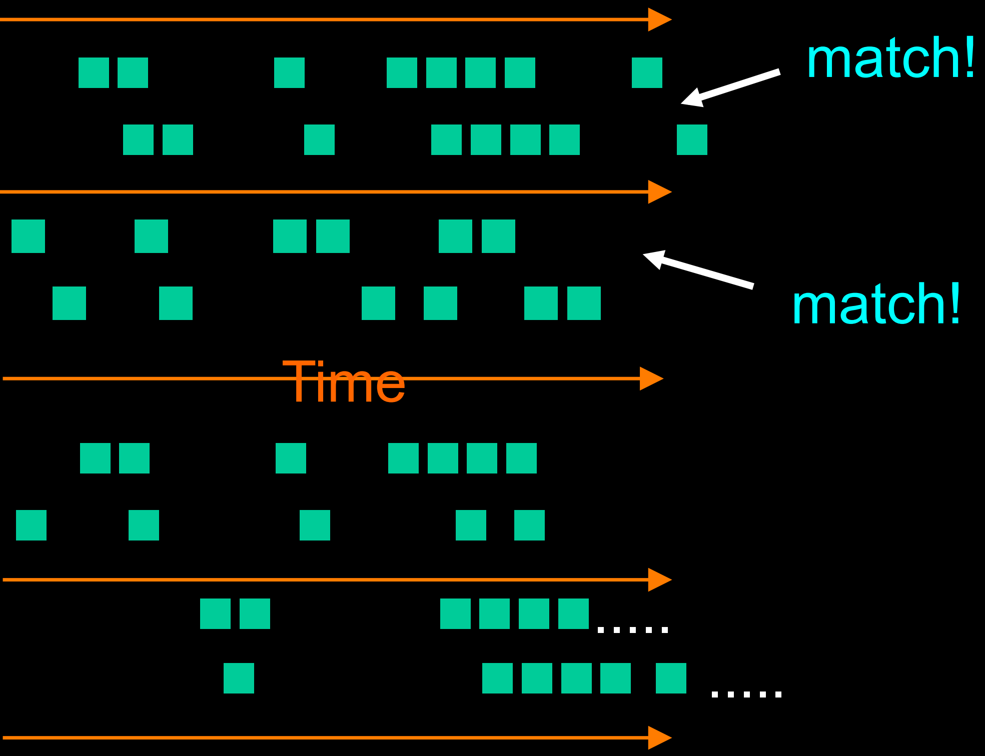
Bob1 gets:

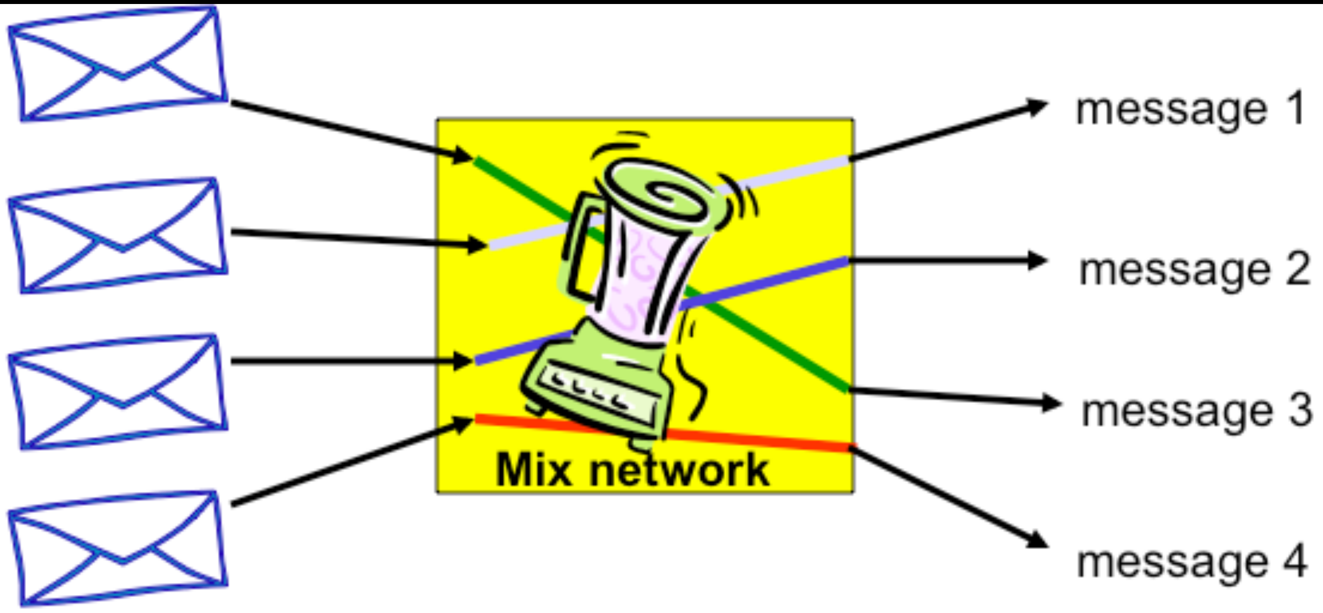
High-latency: Alice1 sends:

Alice2 sends:

Bob1 gets:

Bob2 gets:





Randomly permutes and decrypts inputs

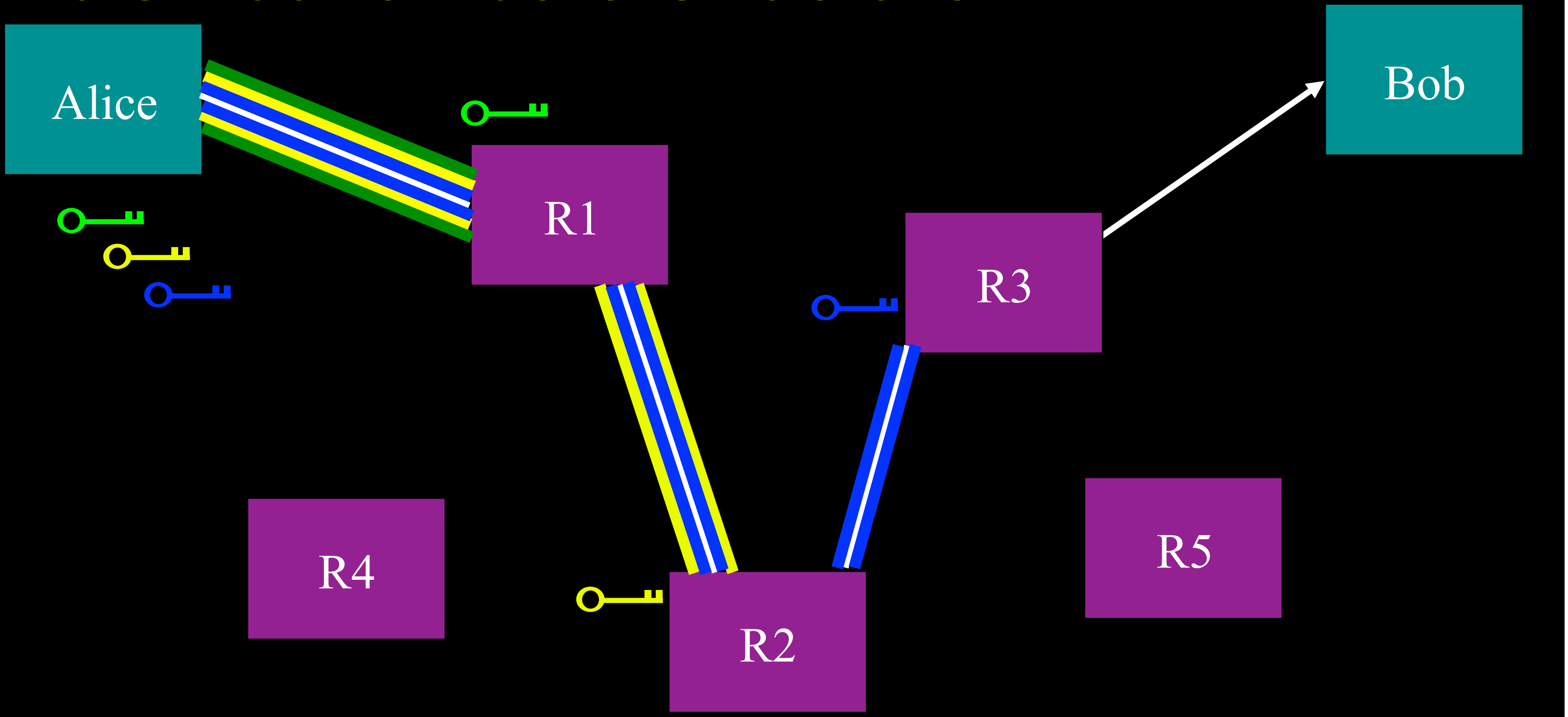
What onion routing is NOT: Mixes

- Entirely different threat model
  - mixes are based on an adversary not being able to correlate inputs and outputs he sees
  - onion routing is based on an adversary not being able to see both inputs and outputs to correlate
  - mix networks more secure against global passive adversary
  - mix networks can be *<u>less secure</u>* vs. local active adversary
- Entirely different communications paradigm: Circuit based encryption vs. per message
  - onion routing supports bidirectional communication
  - onion routing supports low-latency communication
- Can be combined to make mixing onion routers, but not typically done or desired

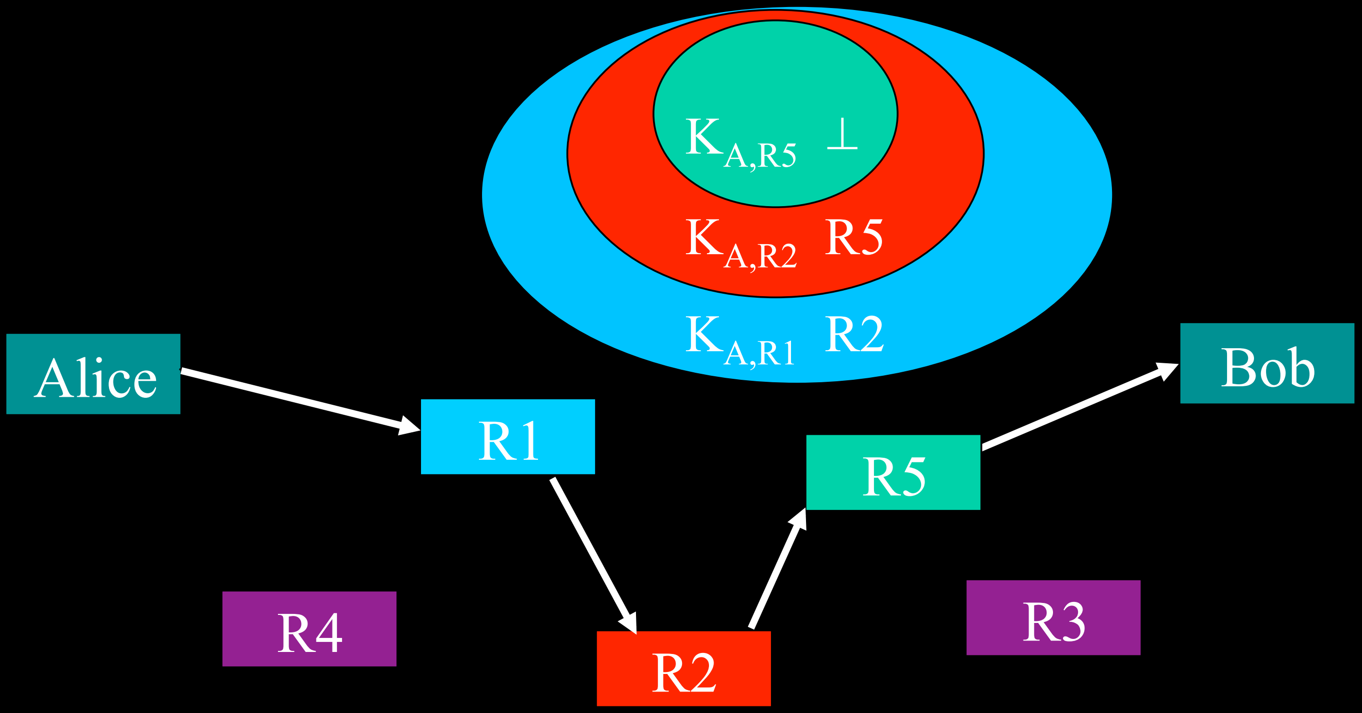
What onion routing is

- Uses expensive crypto (public-key) to lay a cryptographic circuit over which data is passed
- Typically uses free-route circuit building to make location of circuit endpoints unpredictable

Why call it "onion routing"? Answer: Because of the original key distribution data structure

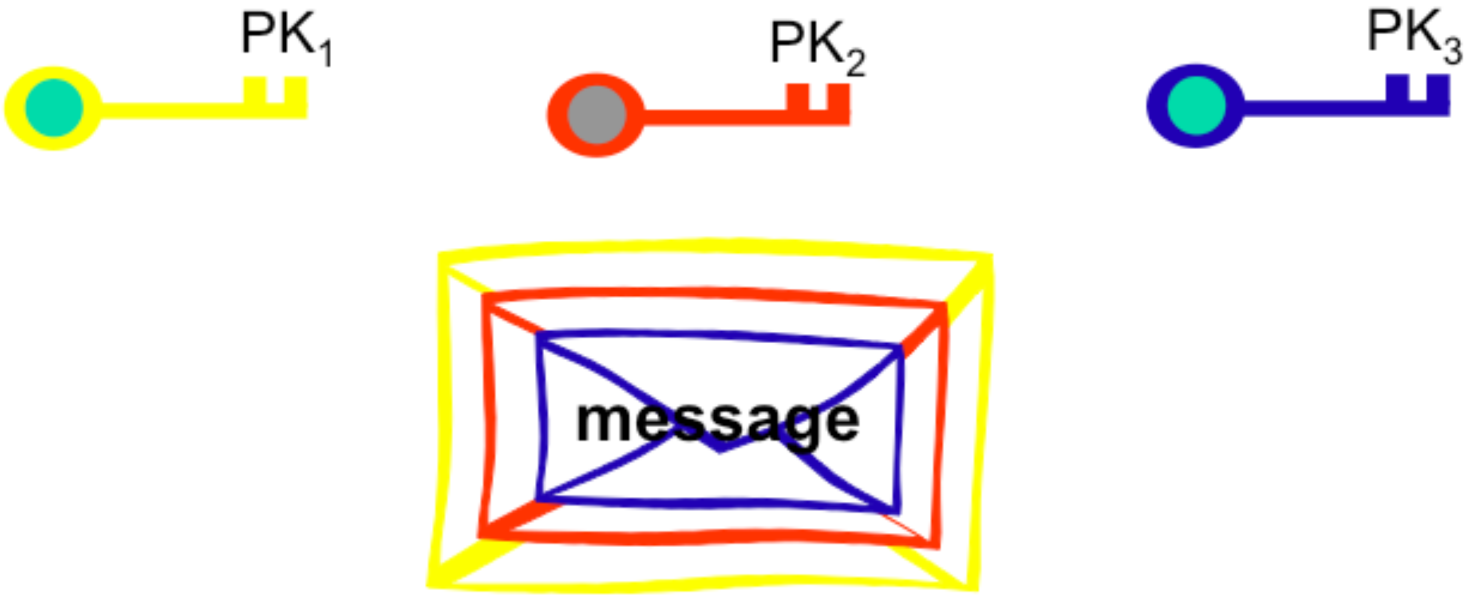


Why is it called onion routing?



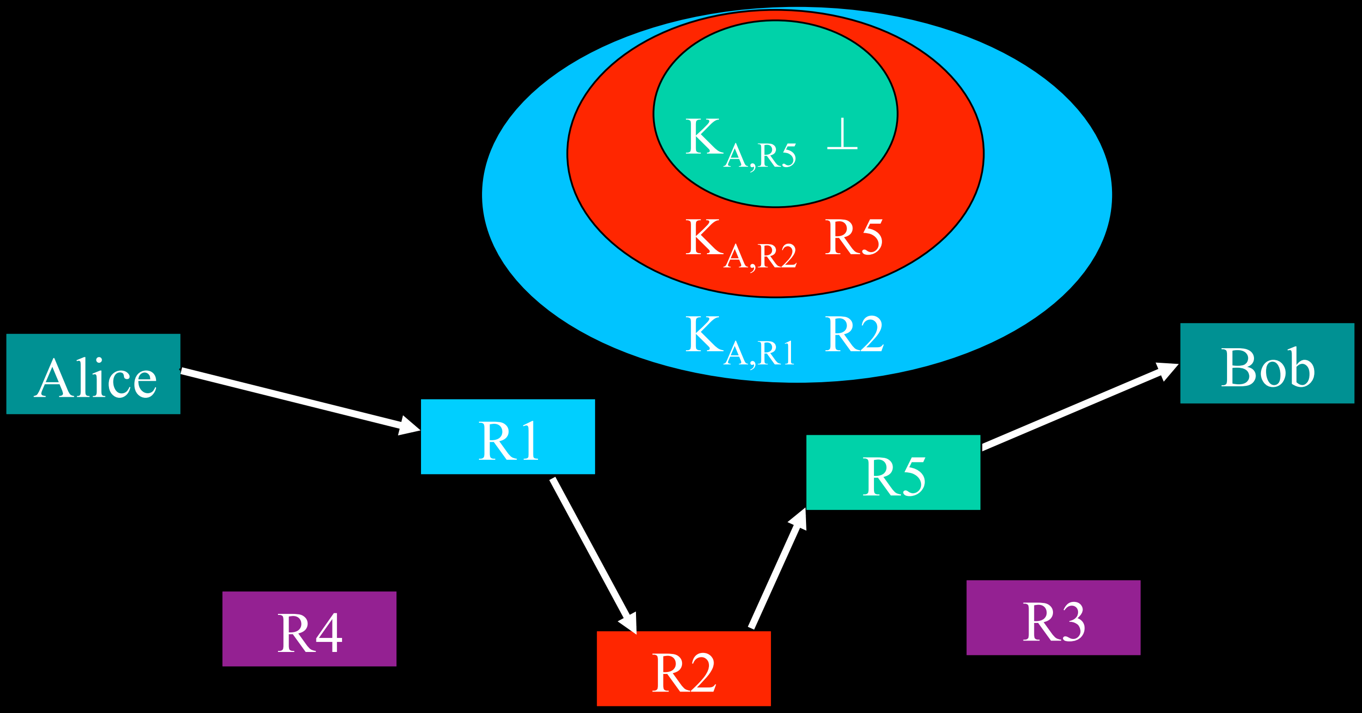
- Onion: Just layers of public-key crypto
  - Nothing in the center, just another layer

Mixi networks have a message in the middle of a public-key “onion”.



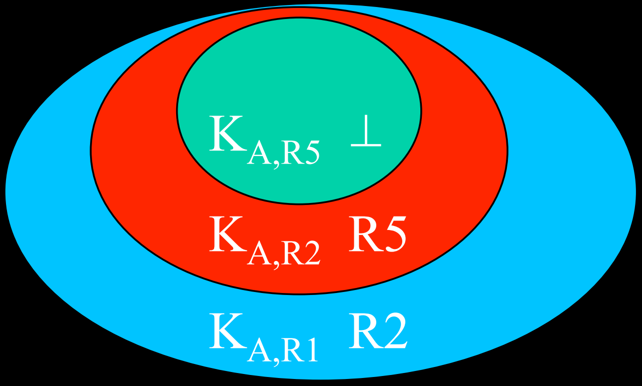
Ciphertext = $E_{PK1}[E_{PK2}[E_{PK3}[\text{message}]]]$

Why is it called onion routing?



- Onion: Just layers of public-key crypto
  - Nothing in the center, just another layer

Circuit setup



- NRL v0 and v1 onion routing and also ZKS Freedom network used onions to build circuits
  - Lacked Forward Secrecy
  - Required storing record of onions against replay
- Tor (NRL v2) uses one layer “onion skins”
  - ephemeral Diffie-Hellman yields forward secrecy
  - No need to record processed onions against replay
  - From suggestion out of Zack Brown’s Cebolla

Aside: Why is it called ‘Tor’ and what does ‘Tor’ mean?

- Frequent question to Roger c. 2001-2: Oh you’re working on onion routing... which one?
- Roger: *THE* onion routing. The original onion routing project from NRL.
- Rachel: That’s a good acronym.
- Roger: And it’s a good recursive acronym.
- Plus, as a word, it has a good meaning in German (door/gate/portal) and Turkish (fine-meshed net)

Aside: Why is it called ‘Tor’ and what does ‘Tor’ mean?

- We foolishly called the first Tor paper “Tor: the second generation onion router”
- But this was very confusing
  - ‘Tor’ stands for “The onion routing” or “Tor’s onion routing”. It does not stand for “the onion router”
  - The paper is about the whole system, not just the onion routers
  - Tor is not the second generation

Aside: Why is it called ‘Tor’ and what does ‘Tor’ mean?

- Tor: A (class of) onion routing design created at NRL starting c. 2001-2.
- Tor: A U.S. 501(c)3 nonprofit organization formed in 2006.
- Tor: A client software program that connects your computer to the Tor network.
- Tor: A volunteer network comprised of c. 3000 nodes serving c. 1 GiB/s data for c. 500K-1M users (see metrics.torproject.org)
- Any amorphous combination of the above or other users

Aside: Why is it called ‘Tor’ and what does ‘Tor’ mean?

Onion routing origins: Generation 0

- Fixed-length five-node circuits
- Integrated configuration
- Static topology
- Loose-source routing
- Partial active adversary
- Rendezvous servers and reply onions

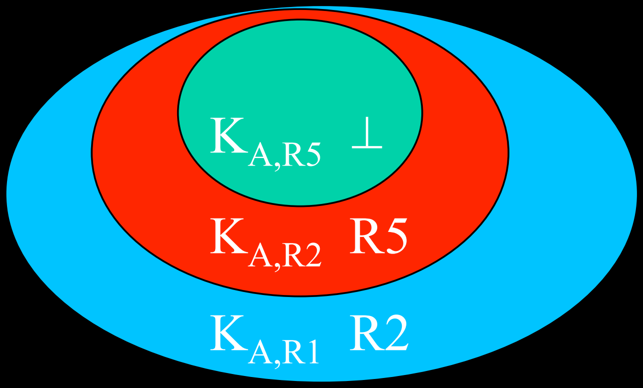
Onion routing, the next generation

- ⋆ Running a client separated from running an OR
- Variable length circuits (up to 11 hops per onion---or tunnel for more)
- Application independent proxies (SOCKS) plus redirector
- ⋆ Entry policies and exit policies
- Dynamic network state, flat distribution of state info
- Multiplexing of multiple application connections in single onion routing circuit
- Mixing of cells from different circuits
- Padding and bandwidth limiting

Third-generation onion routing (Tor)

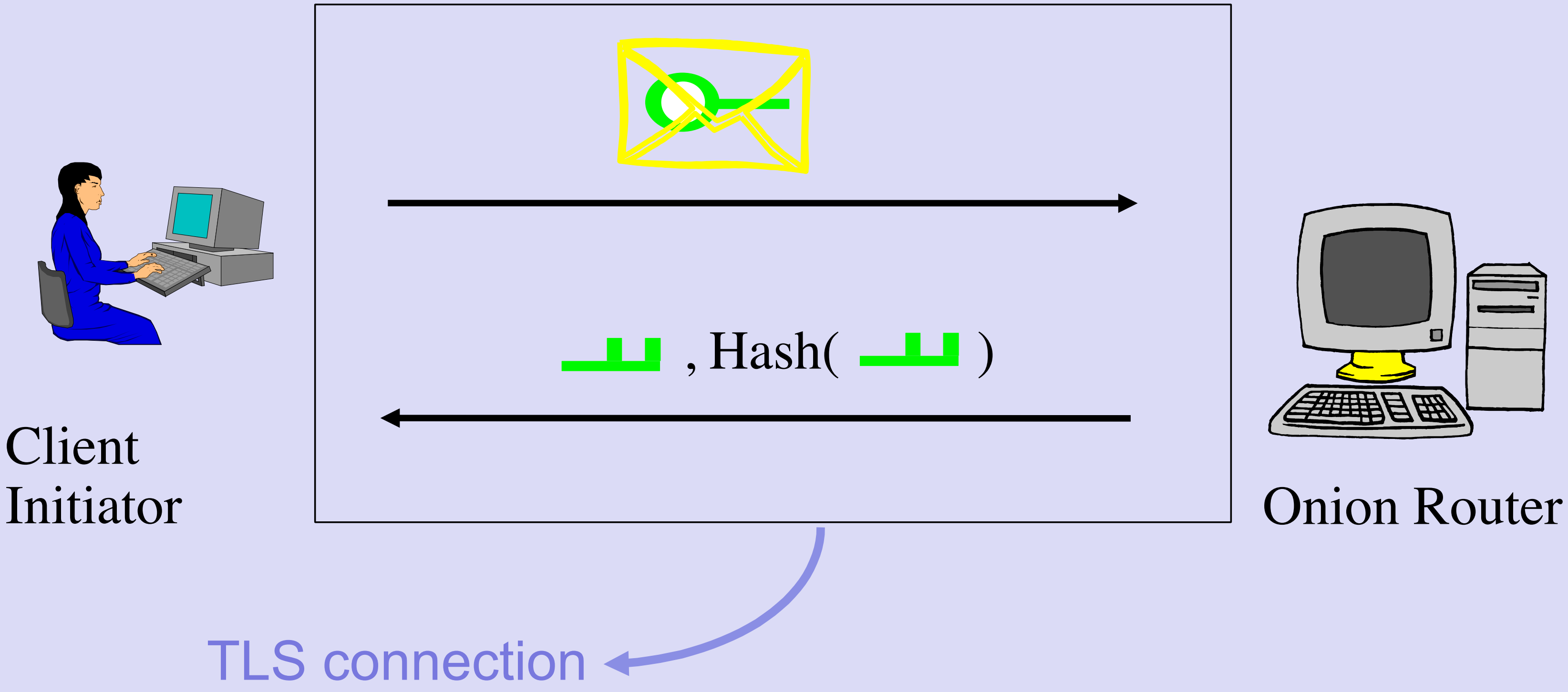
- ⋆ Onion skins, not onions: Diffie-Hellman based circuit building
- Fixed-length three-hop circuits
- Rendezvous circuits and hidden servers
- Directory servers, caching (evolved w/in Tor)
- Most application specific proxies no longer needed (still need e.g. for DNS)
- Congestion control
- End-to-end integrity checking
- No mixing and no padding

Circuit setup



- NRL v0 and v1 onion routing and also ZKS Freedom network used onions to build circuits
  - Lacked Forward Secrecy
  - Required storing record of onions against replay
- Tor (NRL v2) uses one layer “onion skins”
  - ephemeral Diffie-Hellman yields forward secrecy
  - No need to record processed onions against replay
  - From suggestion out of Zack Brown’s Cebolla

Tor Circuit Setup (Create)



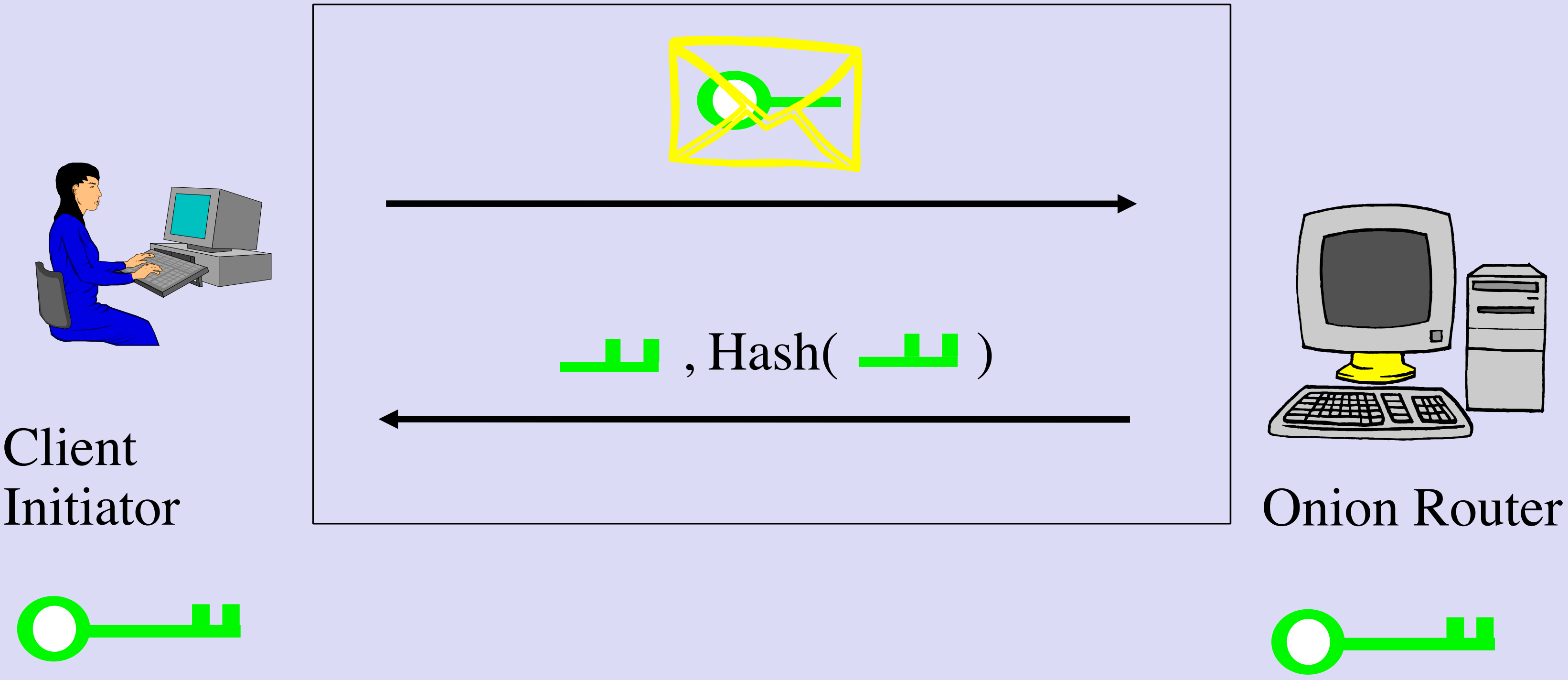
, Hash( )

Client
Initiator

Onion Router

TLS connection

Tor Circuit Setup (Create)

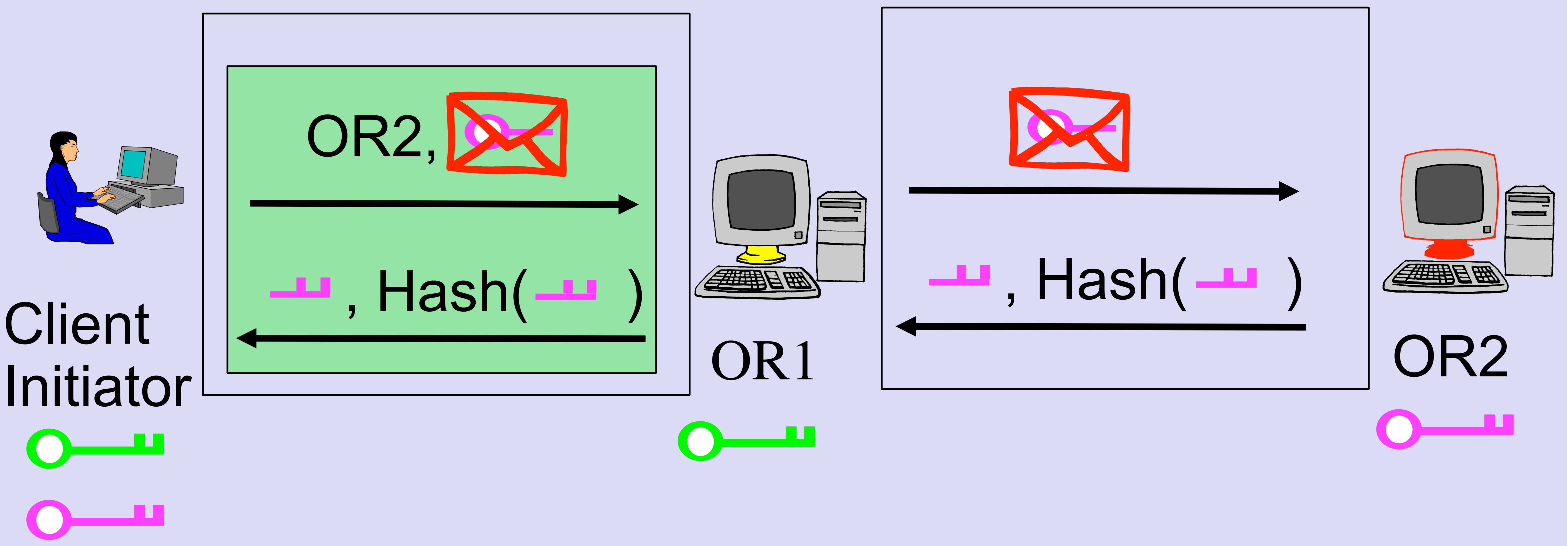


, Hash( )

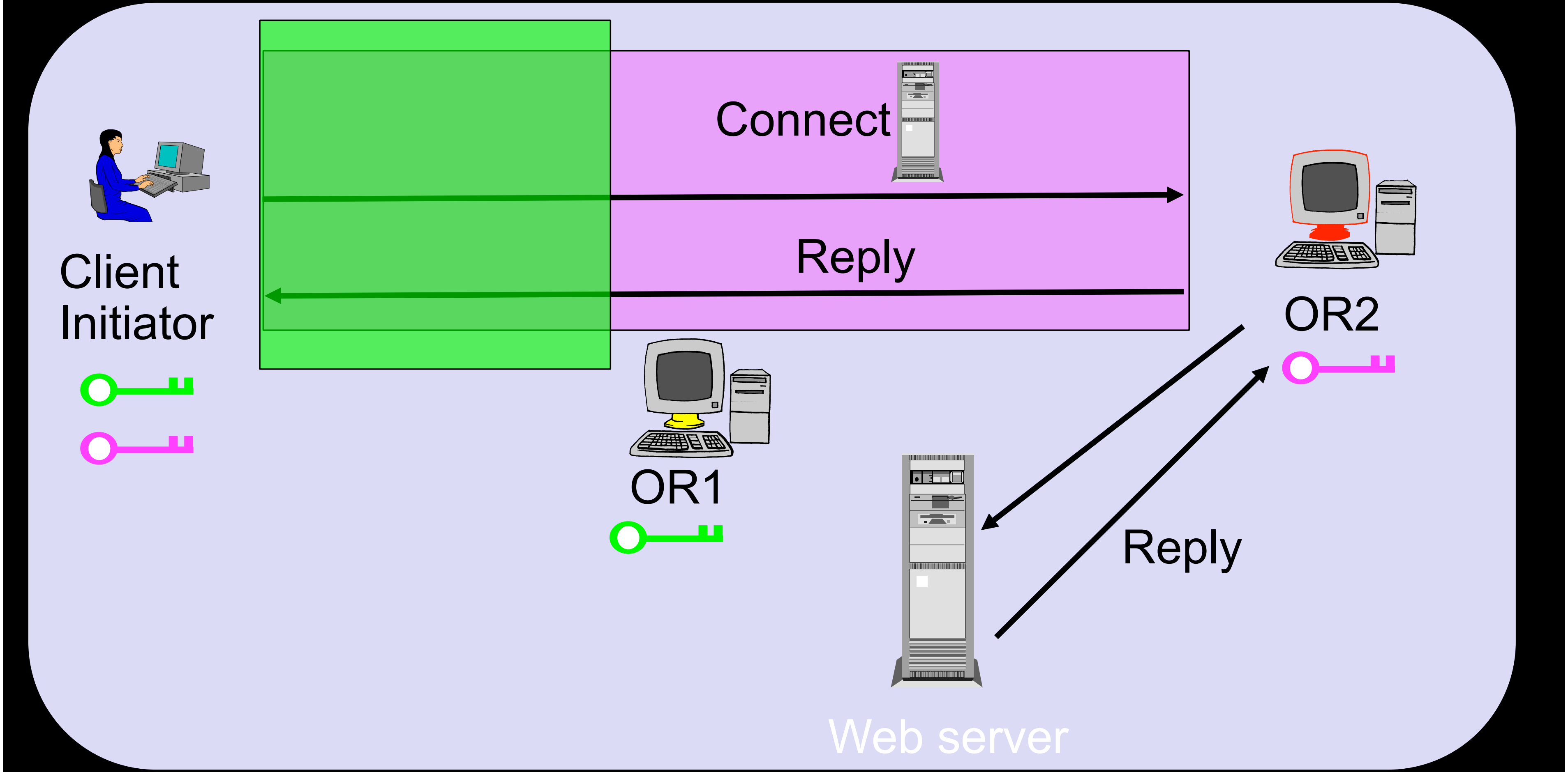
Client
Initiator

Onion Router

Tor Circuit Setup (Extend)



Tor Circuit Setup (Begin) and Data Flow



More on Tor circuit establishment

- Designing your own authentication protocol is error prone. Why not use an established protocol?
- Answer: To fit whole messages inside Tor cells. A public key and a signature don't both fit in one 512-byte cell.
- Protocol was verified using the NRL protocol analyzer in the Dolev-Yao model.
- In 2005 Ian Goldberg found flaw in the way Tor implemented this protocol (checking that a public value was not based on a weak key).
- In 2006 Ian proved the (properly implemented) protocol secure in the random oracle model.

Circuit establishment efficiency

- I and others have proposed protocols to reduce the public-key overhead of circuit establishment.
- Interesting refinements on forward secrecy, but these need more study (and proofs!) before adoption

- Next question: How do we know where to build a circuit?

How do we know where to build a circuit? Network discovery.

- Flat flooding of network state: complex, tricky, scales in principal but ?
- Tor has a directory system
- Originally a single directory signing information about network nodes. Then a multiple redundant directory with mirrors. Then a majority vote system. Then a consensus document system. Then separate things that need to be signed and updated frequently. Then...

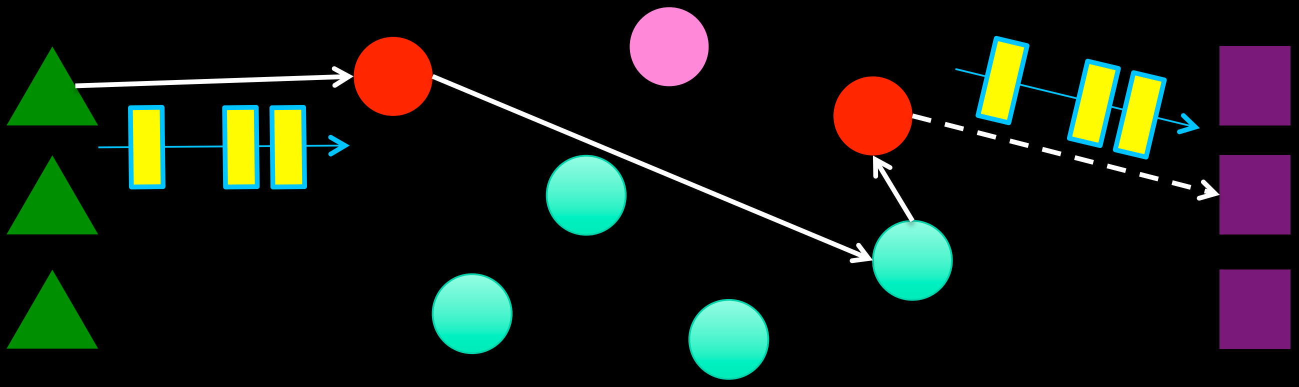
Onion routing was invented to separate identification from routing

- What if onion-routing-network-user is the identification you want to avoid?
- Bridges are proxies into the Tor network that are not publicly listed.
- Tricky to get bridge info out to potential users without giving it to the network blockers.
- See https://blog.torproject.org/blog/research-problems-ten-ways-discover-tor-bridges
- Can also use Telex, Decoy Routing, Cirripede, etc. to inband signal redirection of a cover destination into Tor.

What if adversary owns a botnet or has nation level resources?

- Consumer Alice, abuse/disease victim Alice, local law enforcement Alice, etc. probably OK
- Intelligence analyst Alice, DoD road warrior Alice, etc. ?

First-Last Correlation Problem



What?

- Adversary observes first and last routers.
- Traffic patterns link first and last routers.

Why?

- Attack completely breaks anon *regardless of number of users*.
- Attack possible with moderate resources.
  - 17MB/s compromises random 1% of current Tor users (100 or so home Internet accounts needed for attack)
- Padding, etc. too expensive and will never work anyway.

Key Idea: Trust

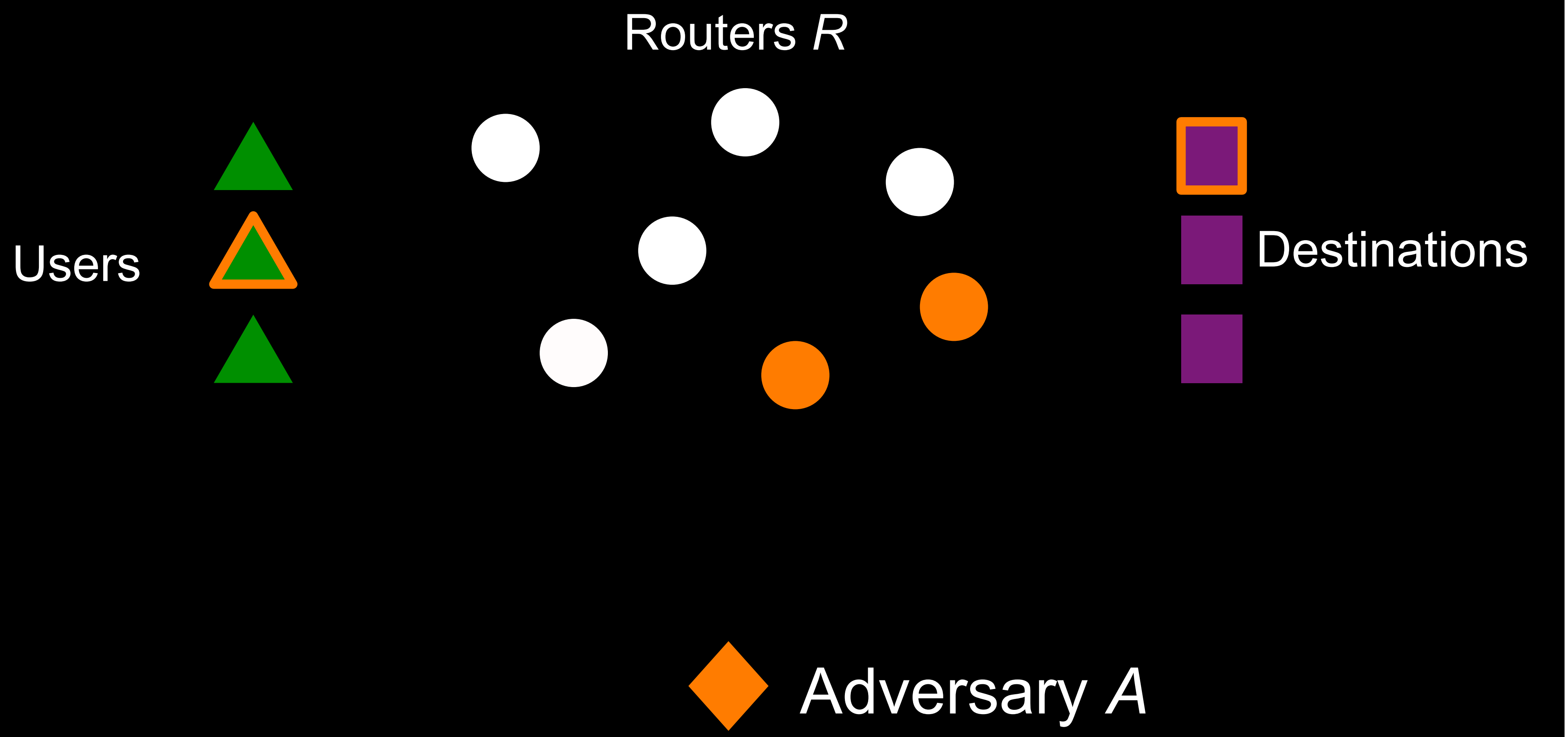
- Users may know how likely a router is to be under observation.

Tor Routers with Possible Trust Factors

Name	Hostname	Bandwidth	Uptime	Location	Tor version	OS
moria	nexico.ediscom.de	4 KB/s	67 days	Germany	0.2.1.26	Linux
Republic	xvm-107.mit.edu	121 KB/s	49 days	USA	0.2.1.29	Linux
Unnamed	static-ip-166-154-142-114.rev.dyxnet.com	58 KB/s	58 days	Hong Kong	0.2.1.29	Windows Server 2003 SP2

Source: http://torstatus.blutmagie.de, 10/12/2011

Basic Adversary Model



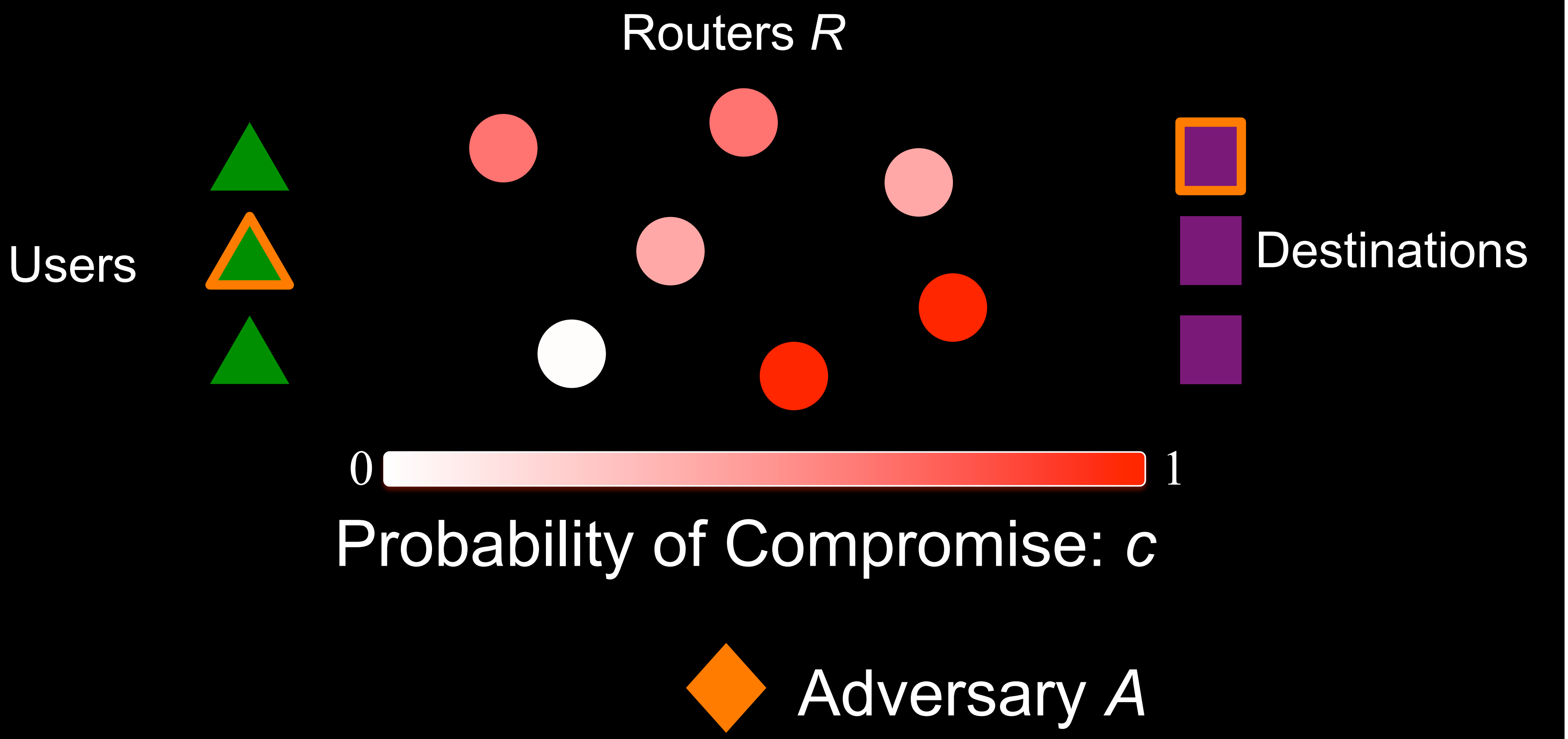
Routers *R*

Users

Destinations

Adversary *A*

Basic *Trust* Model



Routers *R*

Users

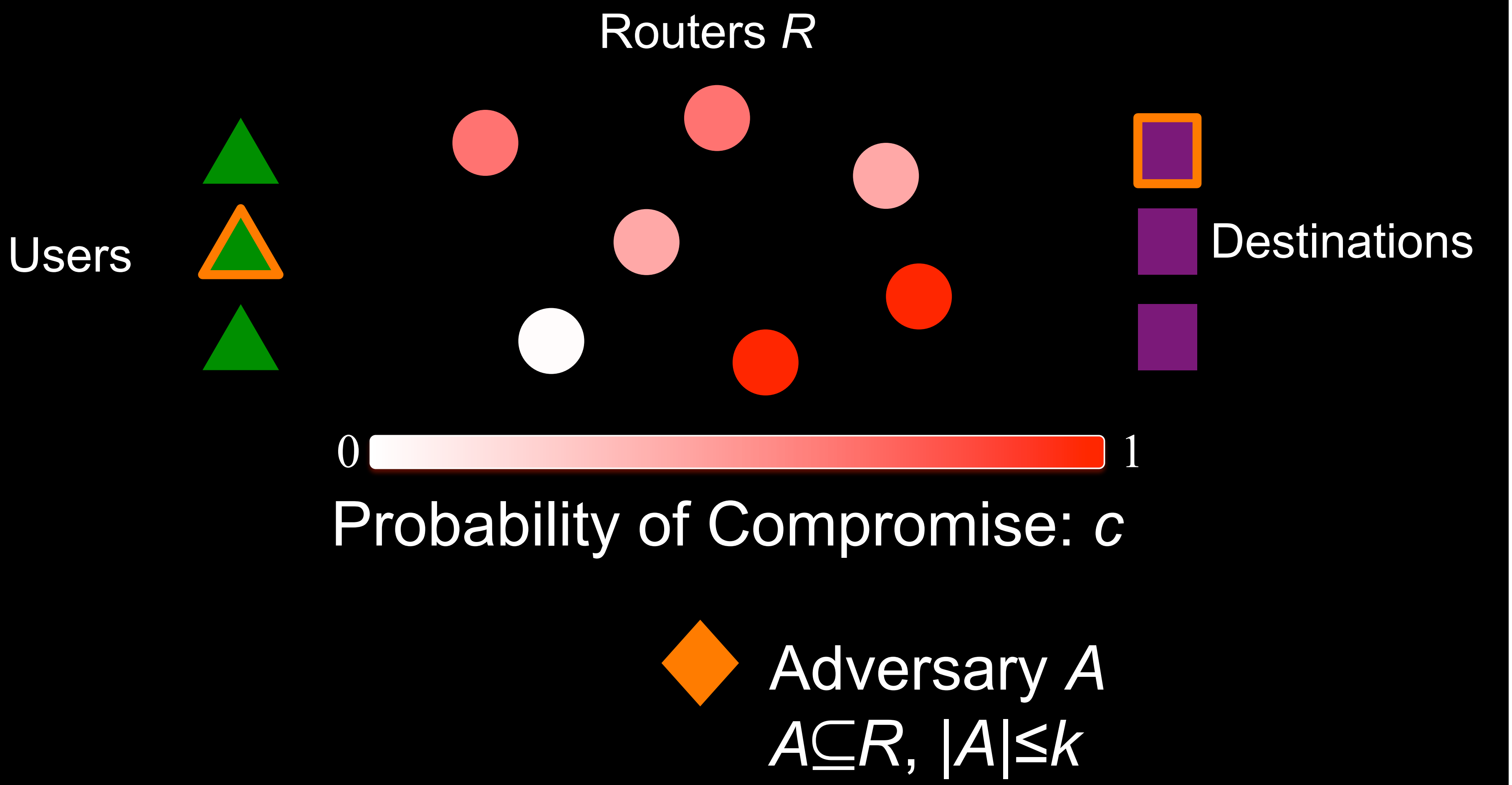
Destinations

0 1

Probability of Compromise: *c*

Adversary *A*

Trust Model 1: Limited Adversary



Routers R

Users

Destinations

0

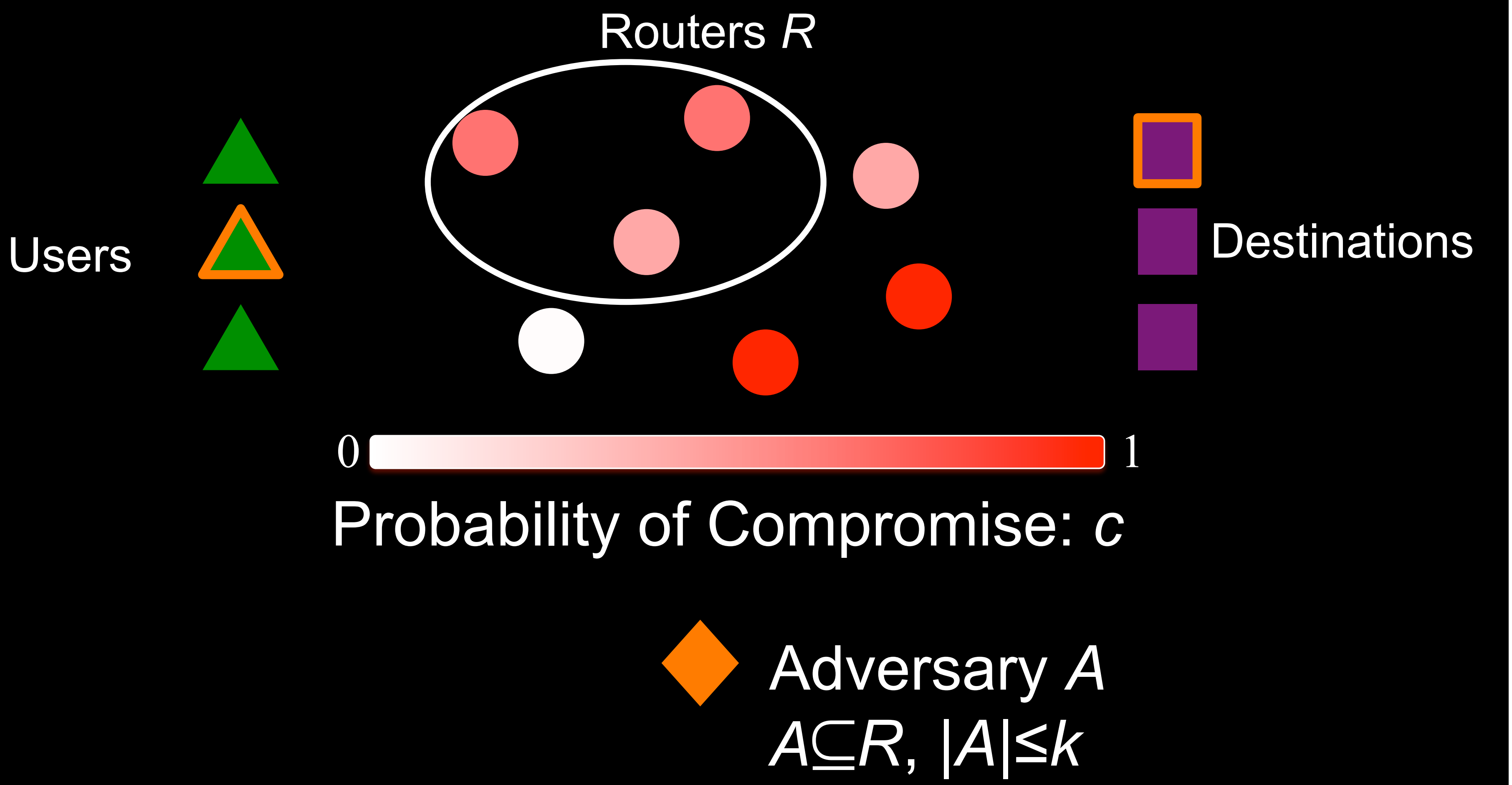
1

Probability of Compromise: c

Adversary A

$A \subseteq R$, $|A| \le k$

Trust Model 1: Limited Adversary

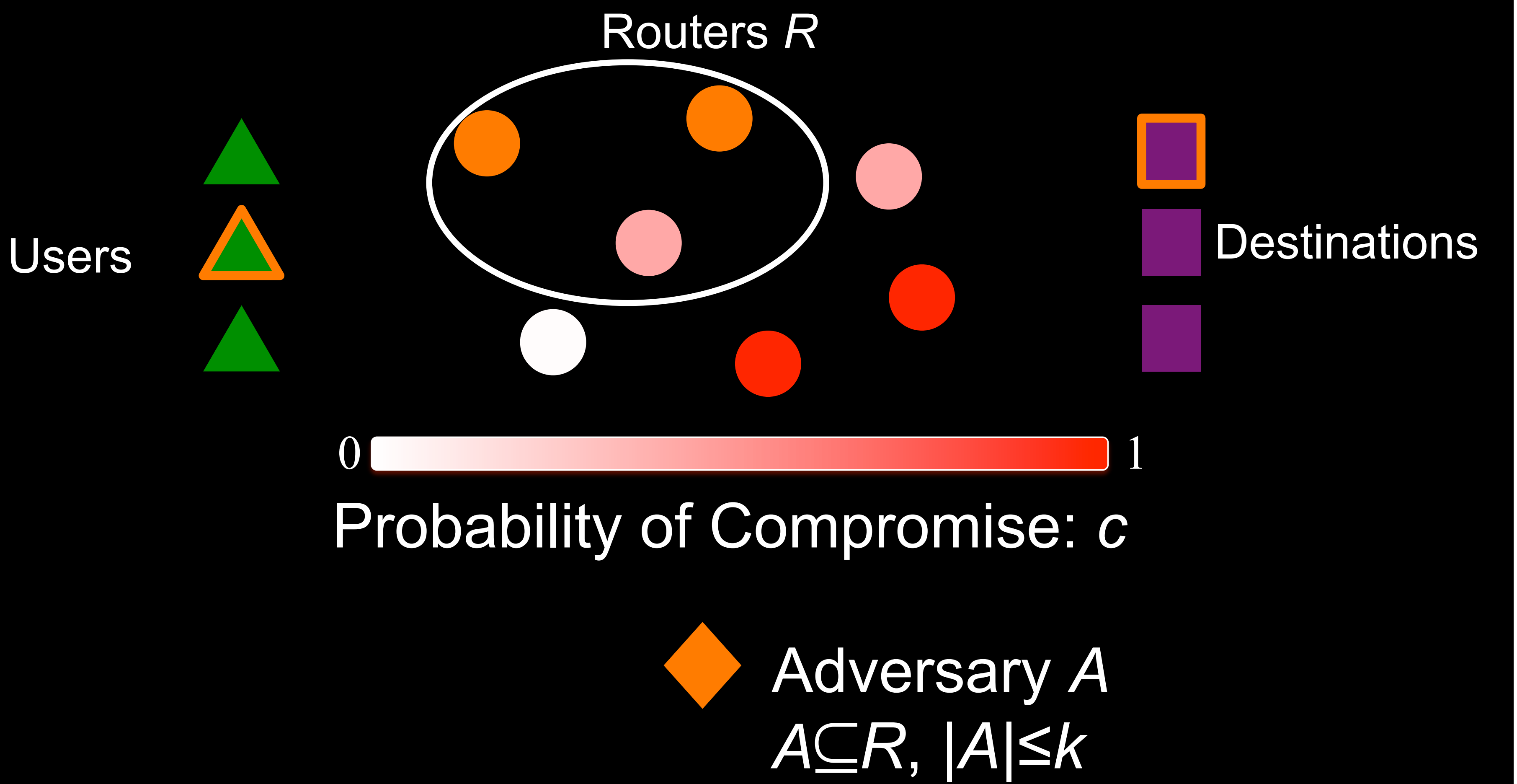


Probability of Compromise: c

Adversary A

$A \subseteq R$, $|A| \leq k$

Trust Model 1: Limited Adversary



Routers *R*

Users

Destinations

0 1

Probability of Compromise: *c*

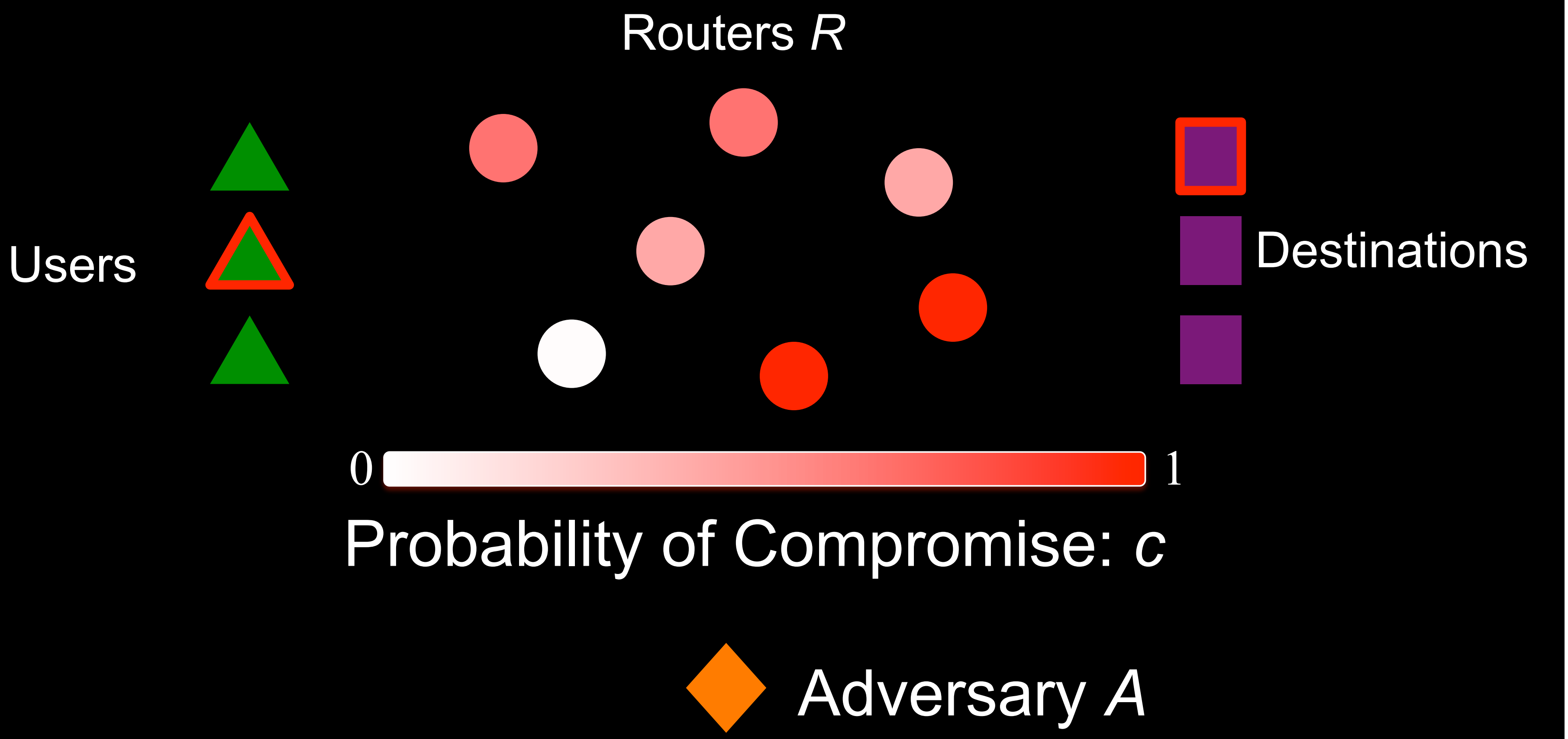
Adversary *A*

$A \subseteq R$, $|A| \leq k$

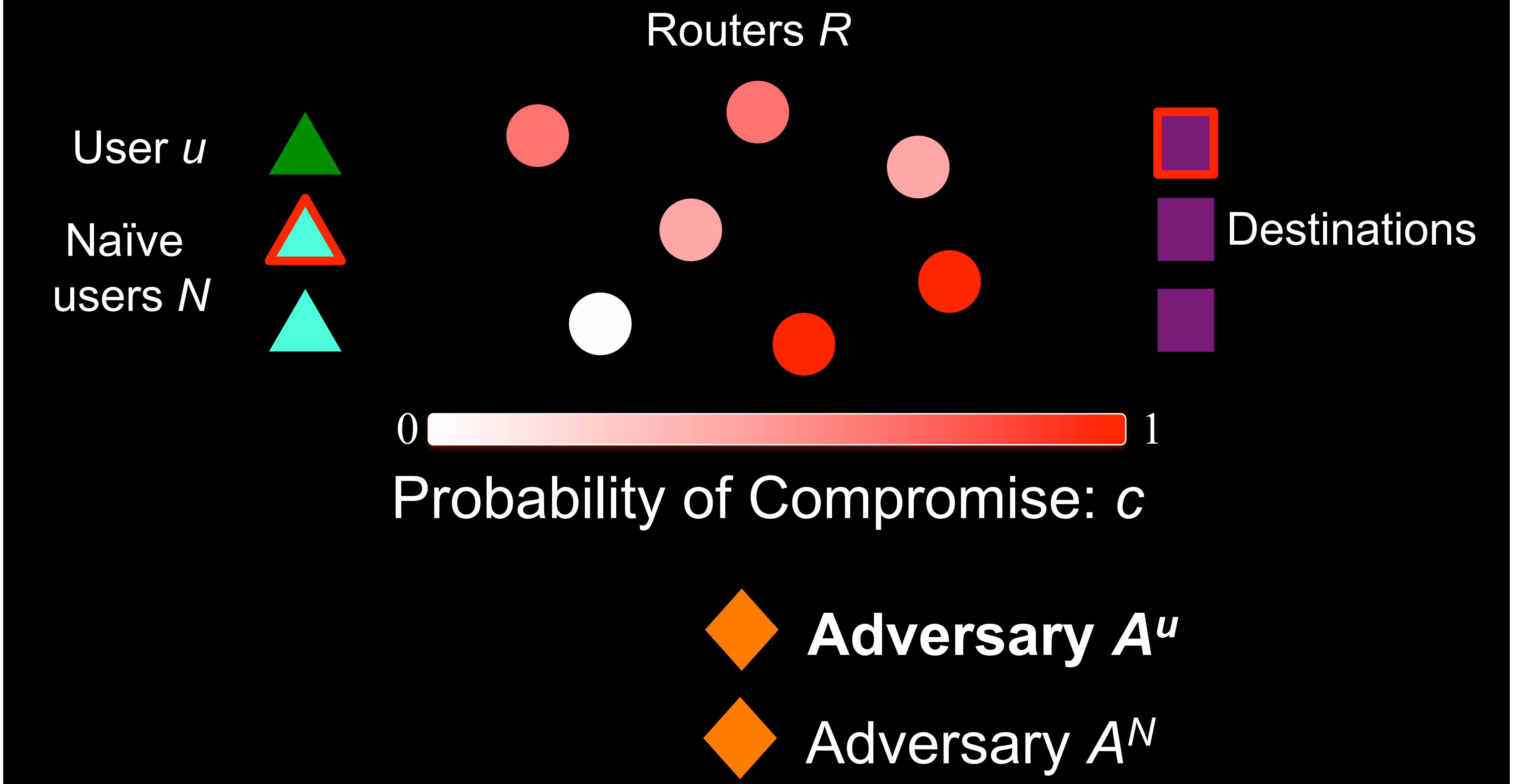
Basic User and Adversary Game

- Router r_i has **trust** t_i. An attempt to compromise a router succeeds with probability $c_i = 1-t_i$.
- Users choose a distribution from which they will select paths.
- Adversary attempts to compromise at most k routers, $K \subseteq R$.
- After attempts, users actually choose paths.

Trust Model 2: Per-User Adversary



Trust Model 2: Per-User Adversary



Routers R

User u

Naïve users N

Destinations

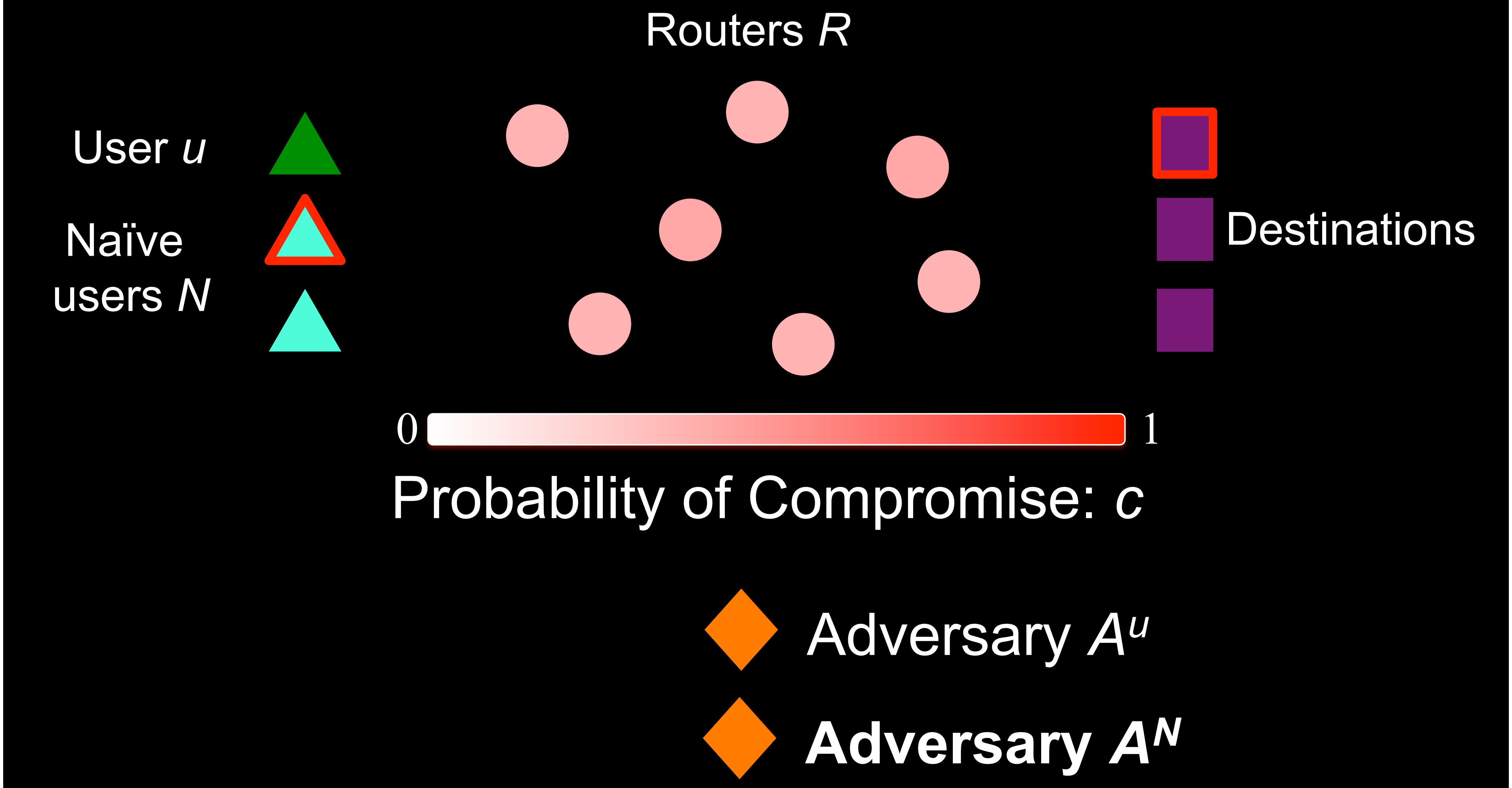
0 1

Probability of Compromise: c

Adversary A^u

Adversary A^N

Trust Model 2: Per-User Adversary



Routers R

User u

Naïve users N

Destinations

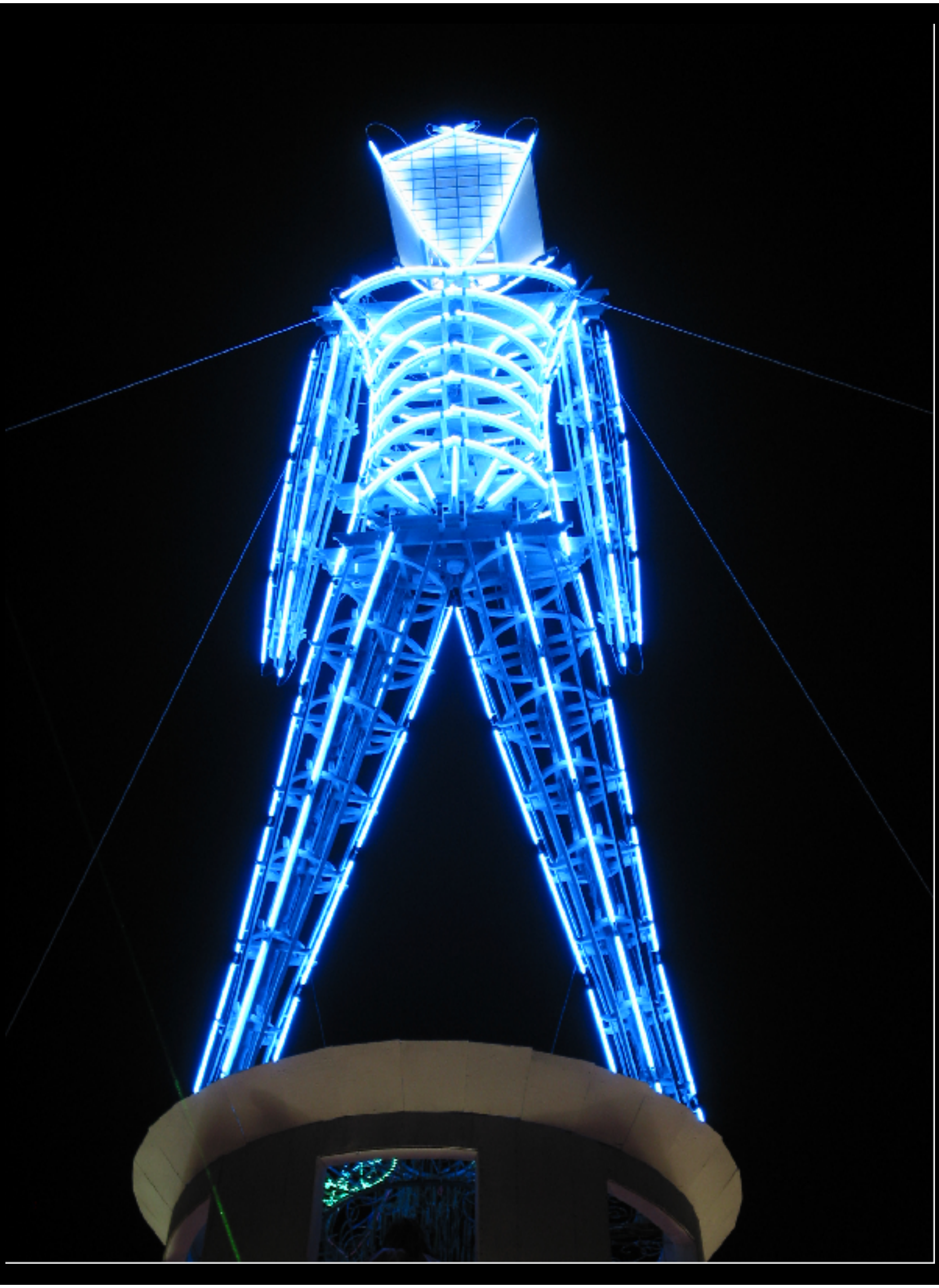
0 1

Probability of Compromise: c

Adversary A^u

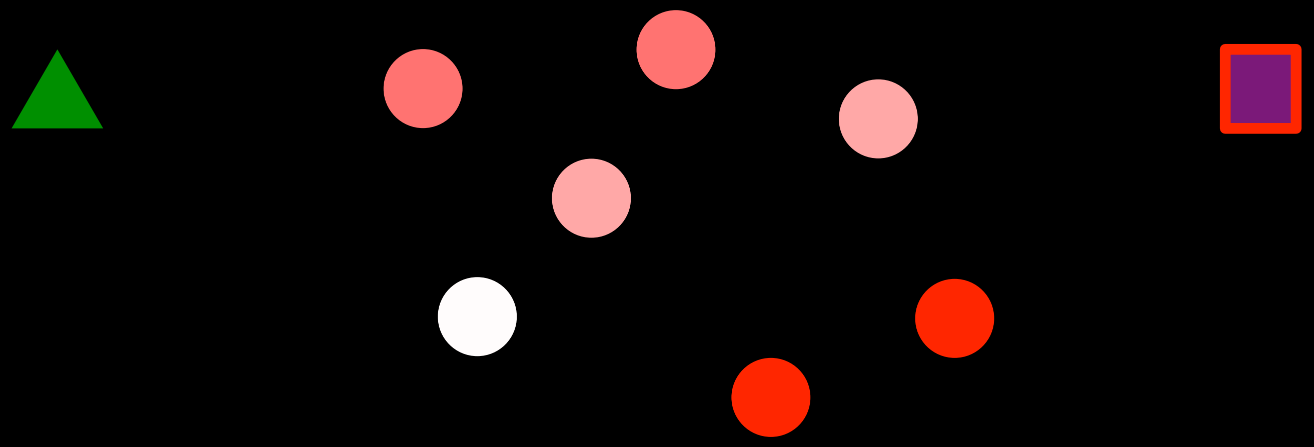
Adversary A^N

The Man



Downhill Algorithm

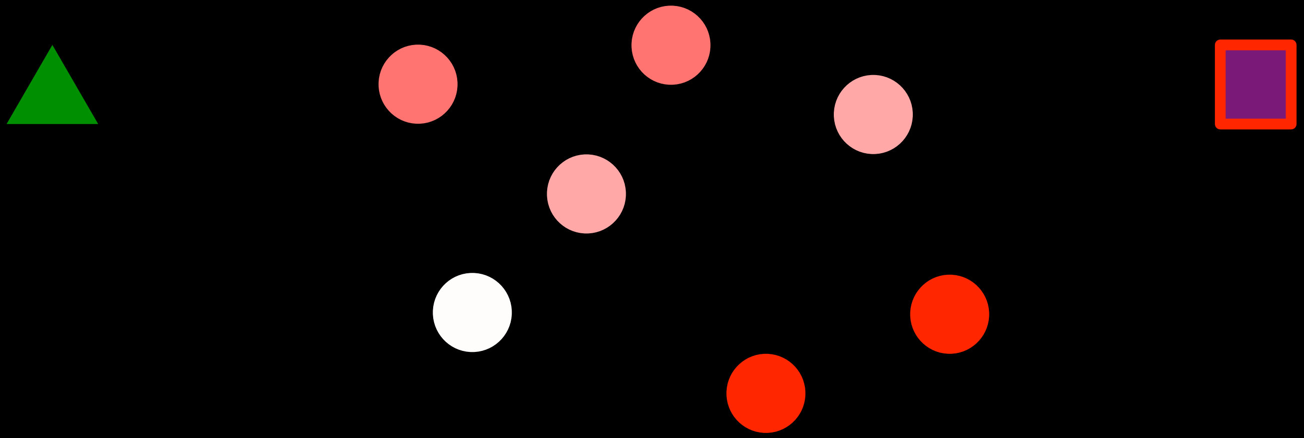
Key idea: Blend in with the naïve users.



1. Set path length *l* and trust levels $\lambda_1,\ldots,\lambda_l$ to optimize anonymity metric.

Downhill Algorithm

Key idea: Blend in with the naïve users.

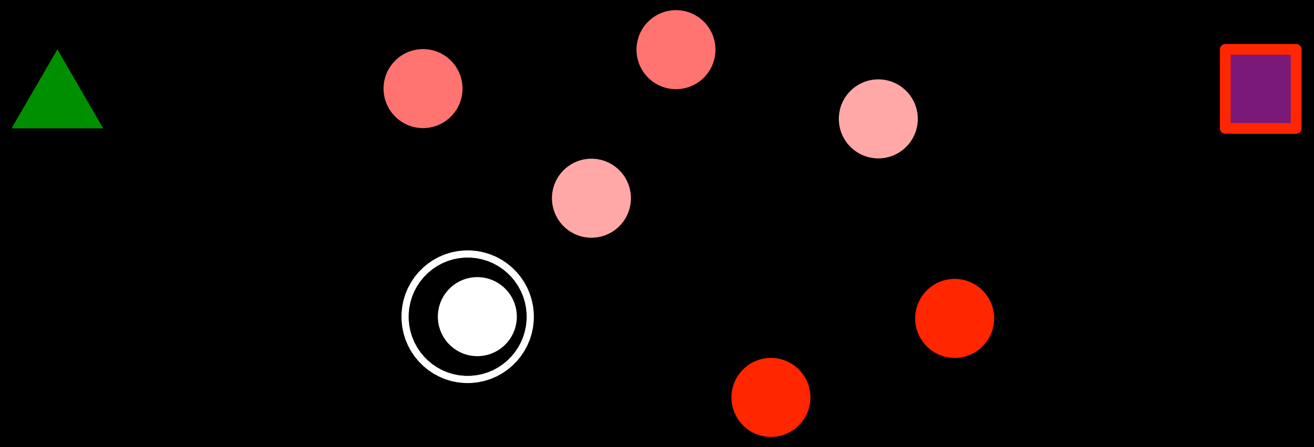


1. Set path length *l* and trust levels $\lambda_1,\ldots,\lambda_l$ to optimize anonymity metric.
2. For $1 \le i \le l$,

   Randomly select among routers with trust $\ge \lambda_i$

Downhill Algorithm

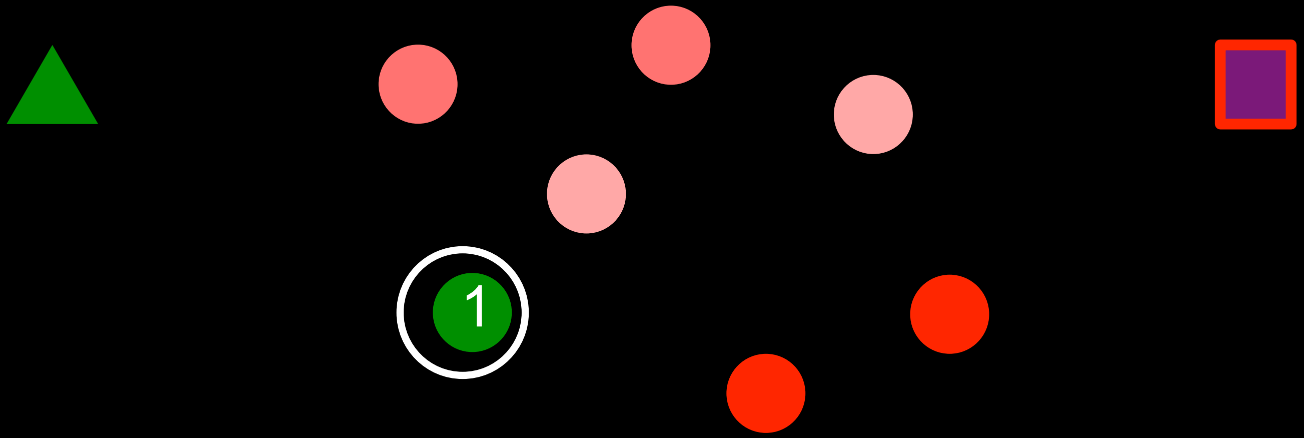
Key idea: Blend in with the naïve users.



1. Set path length *l* and trust levels $\lambda_1,\ldots,\lambda_l$ to optimize anonymity metric.
2. For $1 \le i \le l$,
   Randomly select among routers with trust $\ge \lambda_i$

Downhill Algorithm

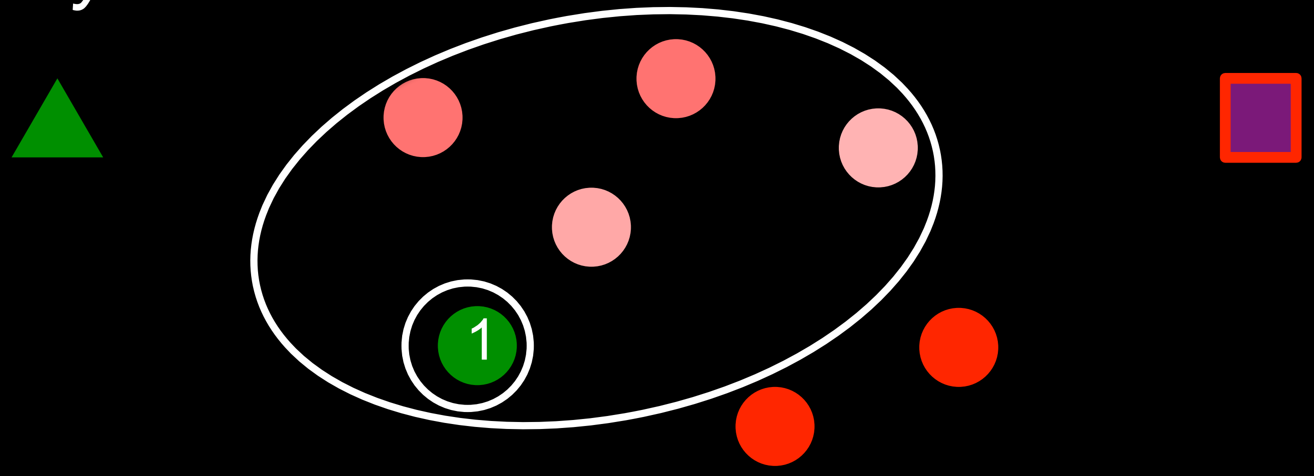
Key idea: Blend in with the naïve users.



1. Set path length l and trust levels $\lambda_1, \ldots, \lambda_l$ to optimize anonymity metric.
2. For $1 \leq i \leq l$,
   Randomly select among routers with trust $\geq \lambda_i$

Downhill Algorithm

Key idea: Blend in with the naïve users.

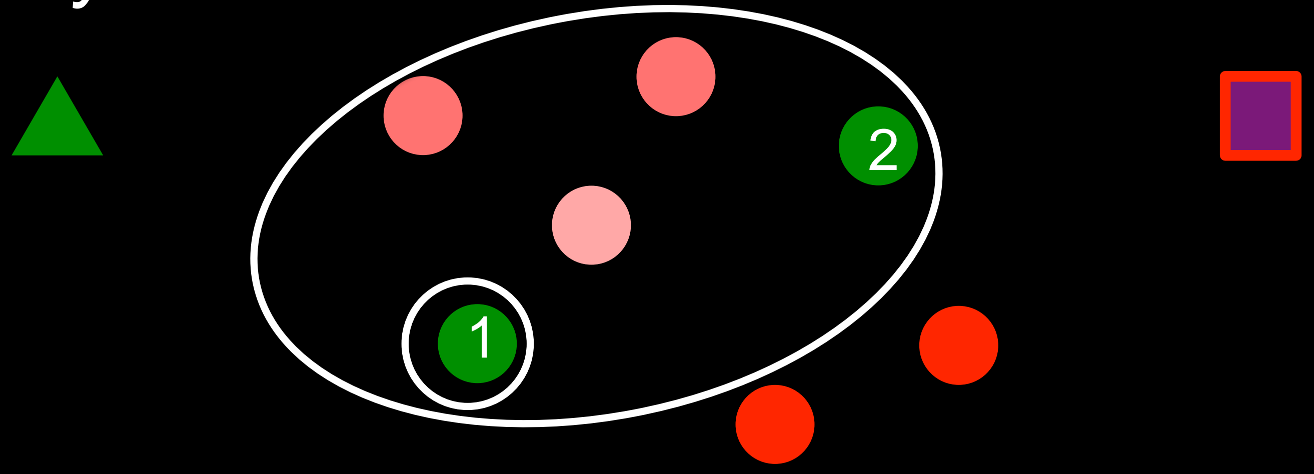


1. Set path length *l* and trust levels $\lambda_1, \ldots, \lambda_l$ to optimize anonymity metric.
2. For $1 \leq i \leq l$,

   Randomly select among routers with trust $\geq \lambda_i$

Downhill Algorithm

Key idea: Blend in with the naïve users.

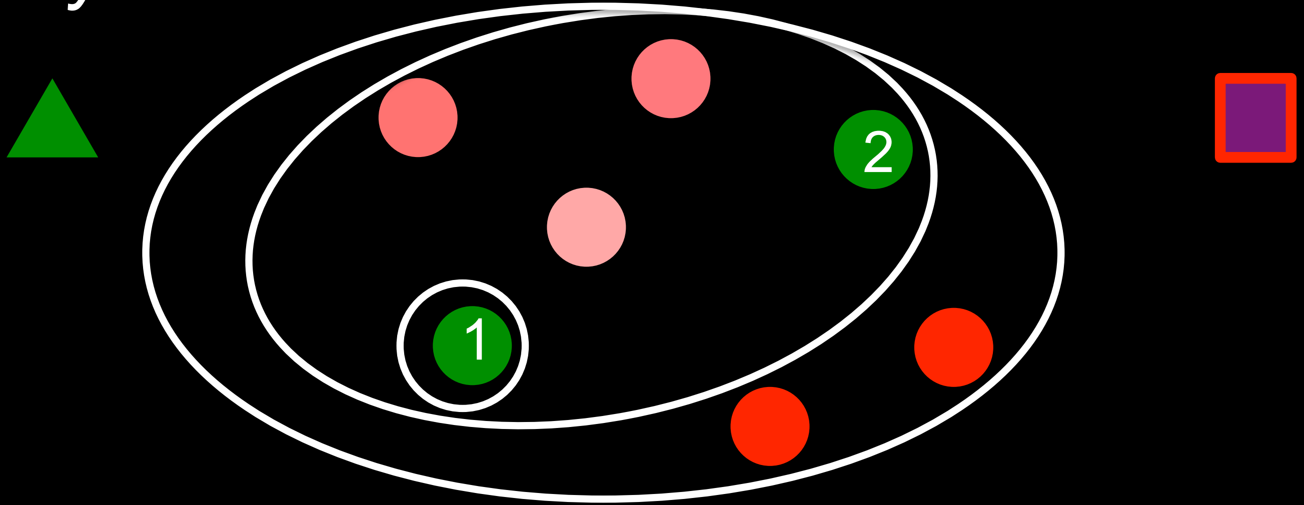


1. Set path length l and trust levels $\lambda_1, \ldots, \lambda_l$ to optimize anonymity metric.
2. For $1 \leq i \leq l$,

   Randomly select among routers with trust $\geq \lambda_i$

Downhill Algorithm

Key idea: Blend in with the naïve users.

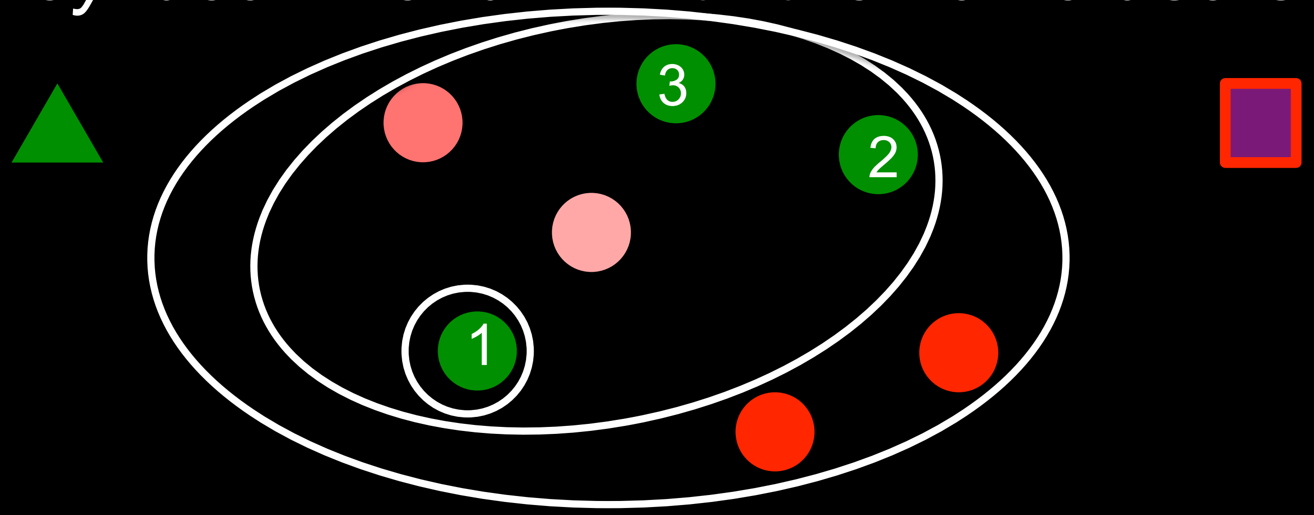


1. Set path length *l* and trust levels $\lambda_1,\ldots,\lambda_l$ to optimize anonymity metric.
2. For $1 \leq i \leq l$,

   Randomly select among routers with trust $\geq \lambda_i$

Downhill Algorithm

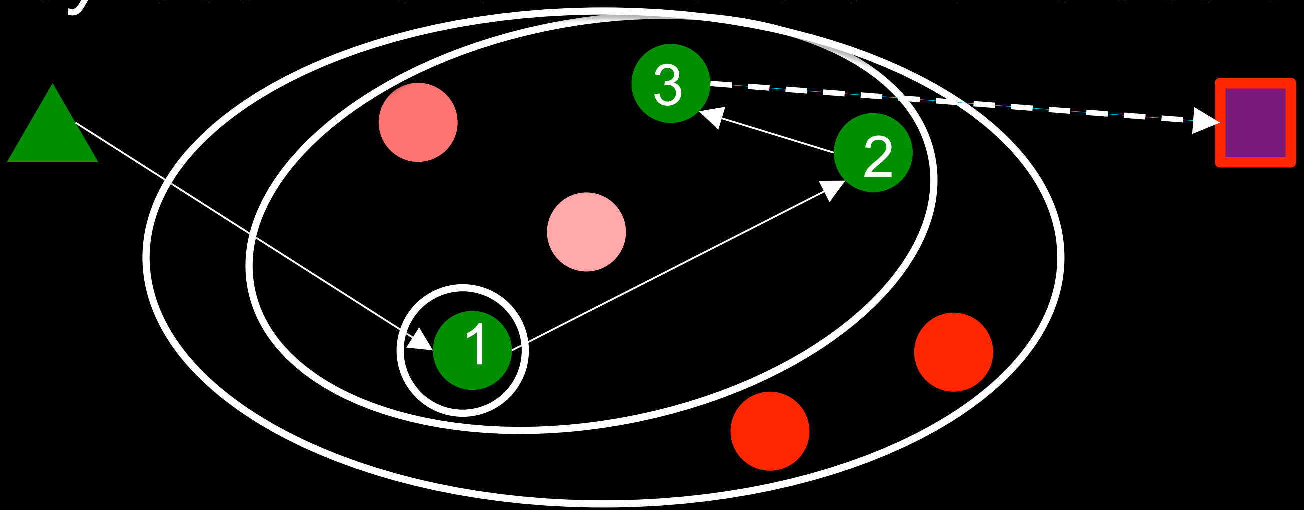
Key idea: Blend in with the naïve users.



1. Set path length *l* and trust levels $\lambda_1, \ldots, \lambda_l$ to optimize anonymity metric.
2. For $1 \leq i \leq l$,
   Randomly select among routers with trust $\geq \lambda_i$

Downhill Algorithm

Key idea: Blend in with the naïve users.



1. Set path length *l* and trust levels $\lambda_1, \ldots, \lambda_l$ to optimize anonymity metric.
2. For $1 \le i \le l$,
   Randomly select among routers with trust $\ge \lambda_i$
3. For each connection,
   Create circuit through selected routers to the destination.

Anonymity Analysis

Metric: Posterior probability of actual source of a given connection.

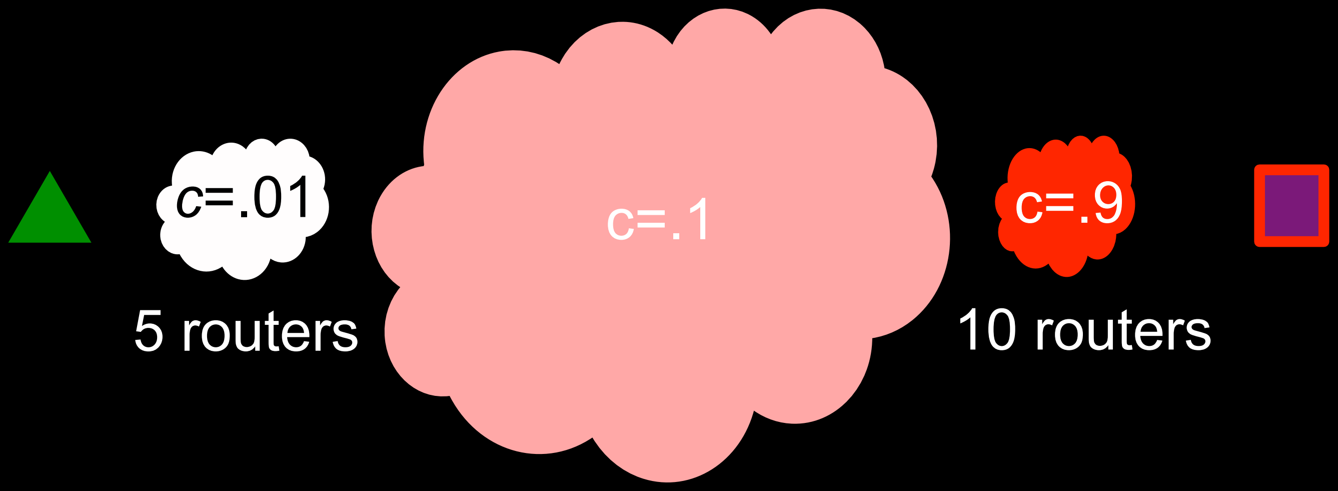
Expected anonymity	Downhill	Most trusted	Random	Lower bound
Many @ medium trust	0.0274	0.2519	0.1088	0.01
Many @ low trust	0.0550	0.1751	0.4763	0.001

Anonymity Analysis

Metric: Posterior probability of actual source of a given connection.

Expected anonymity	Downhill	Most trusted	Random	Lower bound
Many @ medium trust	0.0274	0.2519	0.1088	0.01
Many @ low trust	0.0550	0.1751	0.4763	0.001

Scenario 1: User has some limited information.



c=.01

5 routers

c=.1

1000 routers

c=.9

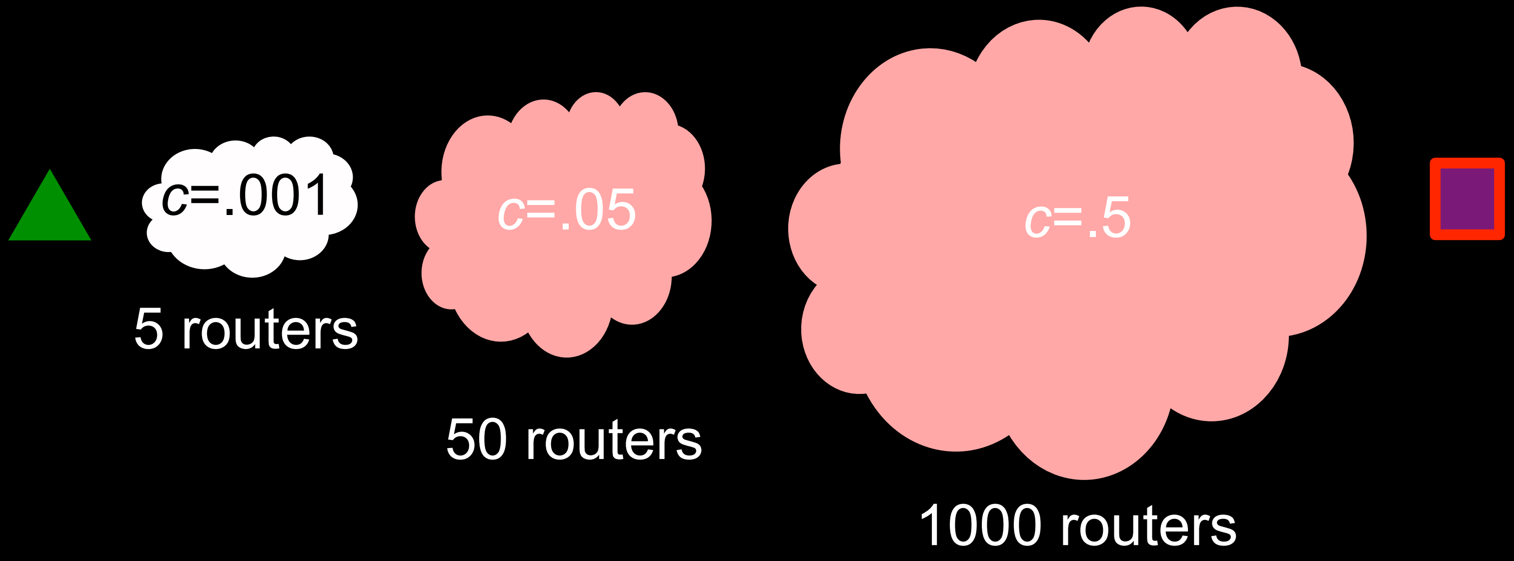
10 routers

Anonymity Analysis

Metric: Posterior probability of actual source of a given connection.

Expected anonymity	Downhill	Most trusted	Random	Lower bound
Many @ medium trust	0.0274	0.2519	0.1088	0.01
Many @ low trust	0.0550	0.1751	0.4763	0.001

Scenario 2: User and friends run routers. Adversary is strong.



Using Trust is first approach to protect traffic even if adversary owns a large chunk of the network.

Not yet (or much) mentioned/future work:

- Datagram transport
- Links
- Performance/congestion/throttling/incentives
- Hidden services
- Trust propagation
- Better security models

Questions?