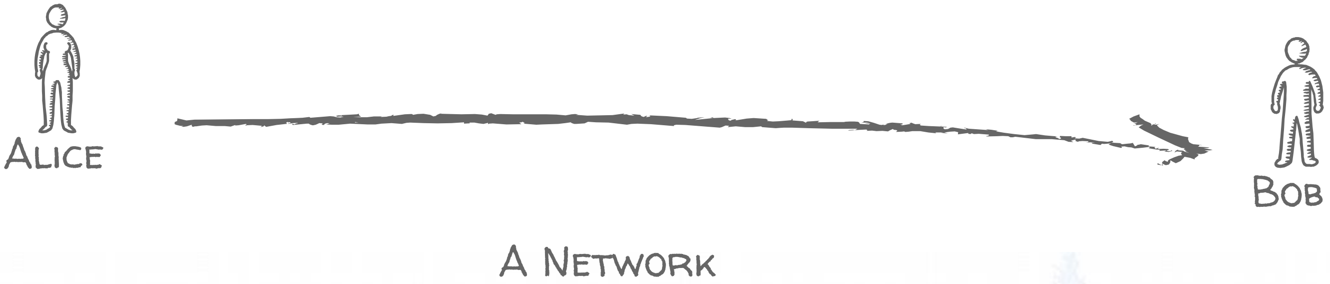
Dissecting Tor Bridges
A Security Evaluation of their Private and Public Infrastructures

Srdjan Matic, Carmela Troncoso, Juan Caballero

Dublin
31 March 2017

Privacy in electronic communications

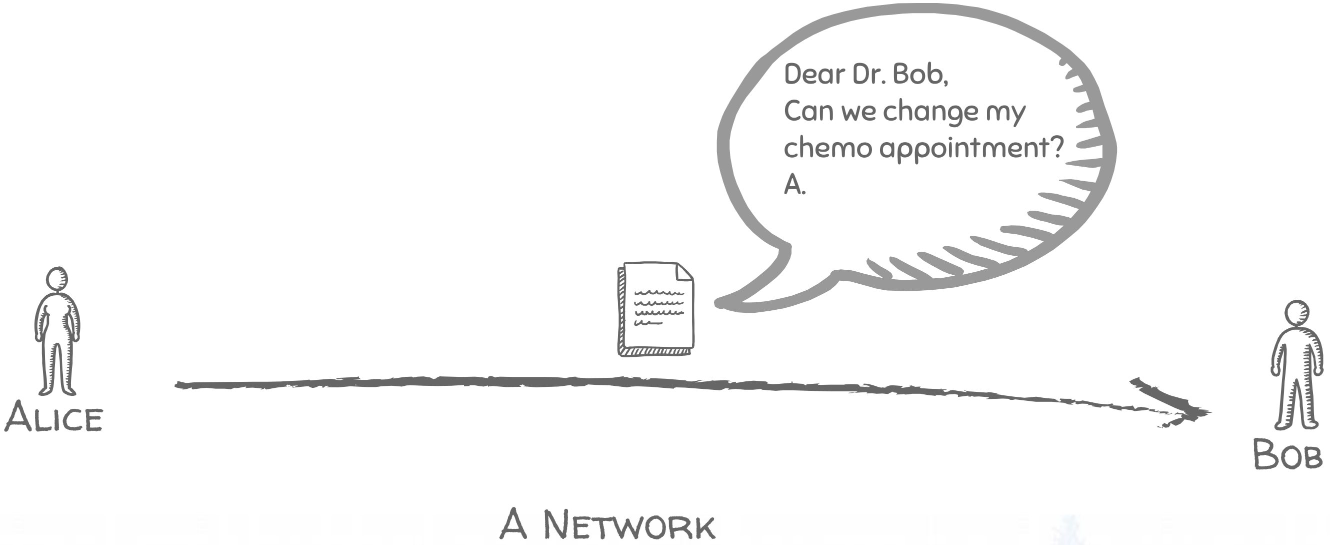


Alice

Bob

A Network

Privacy in electronic communications



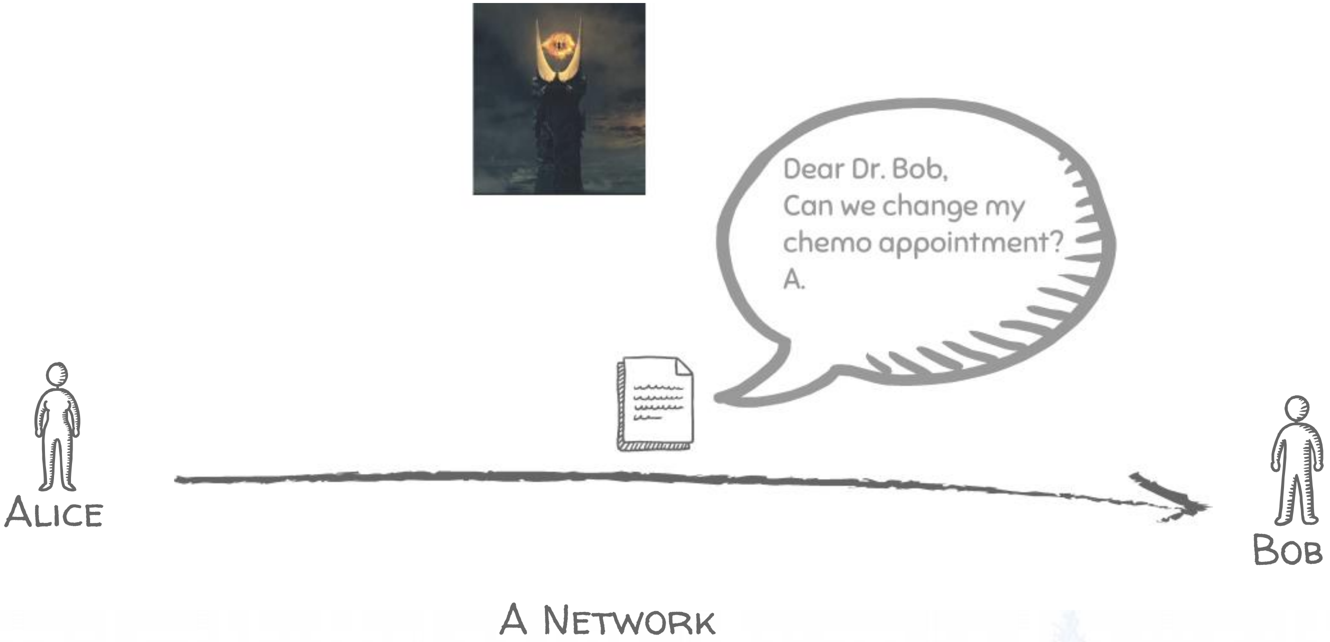
Dear Dr. Bob,
Can we change my
chemo appointment?
A.

Alice

Bob

A Network

Privacy in electronic communications



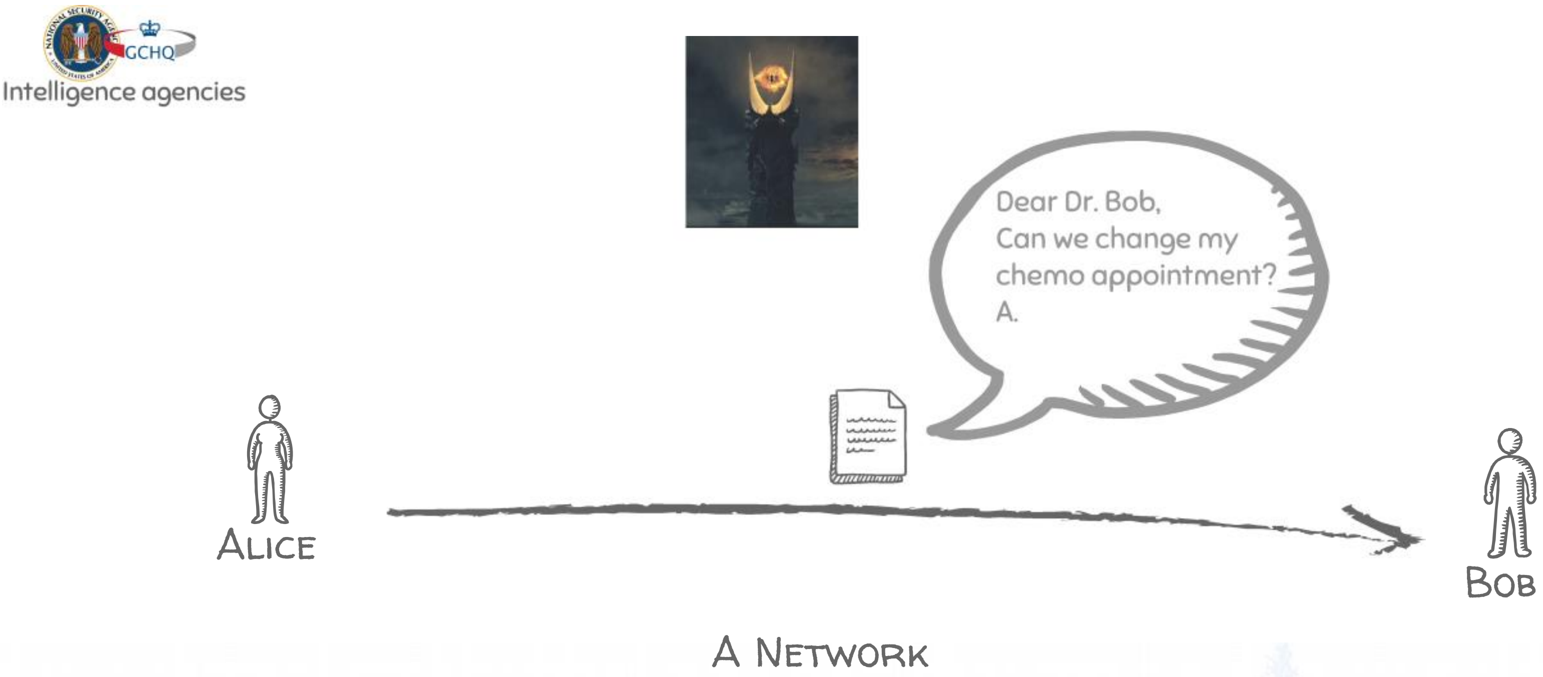
Dear Dr. Bob,
Can we change my chemo appointment?
A.

Alice

Bob

A Network

Privacy in electronic communications



Intelligence agencies

Dear Dr. Bob,
Can we change my chemo appointment?
A.

Alice

Bob

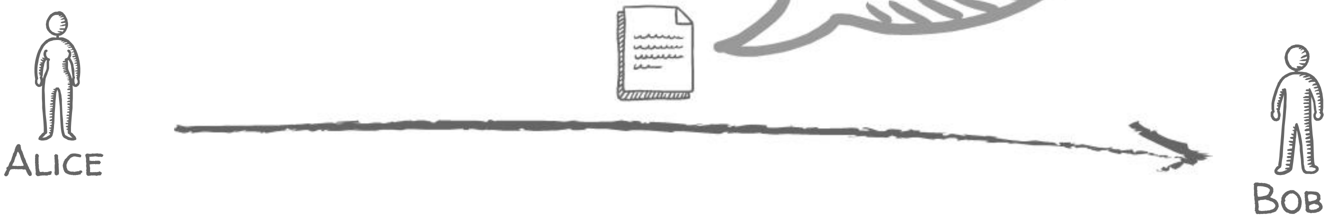
A Network

Privacy in electronic communications

Intelligence agencies

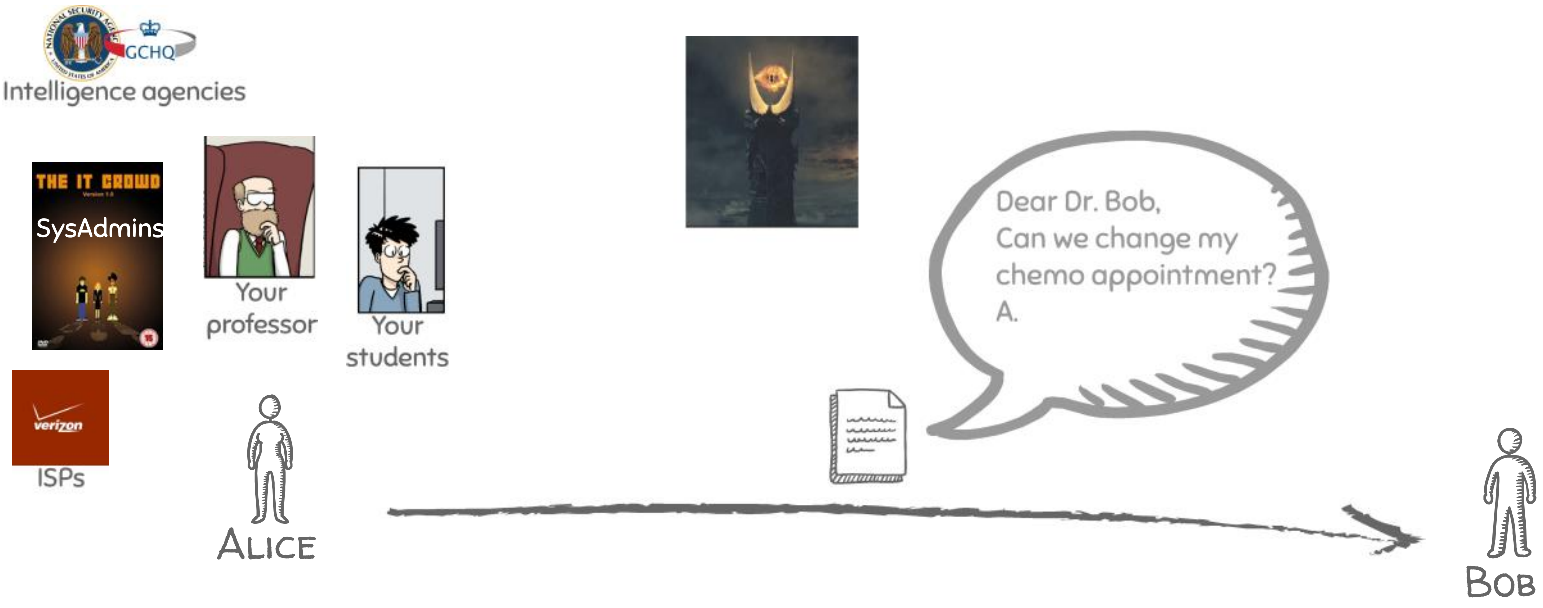
ISPs

Dear Dr. Bob,
Can we change my
chemo appointment?
A.



A Network

Privacy in electronic communications



Intelligence agencies

SysAdmins

Your professor

Your students

ISPs

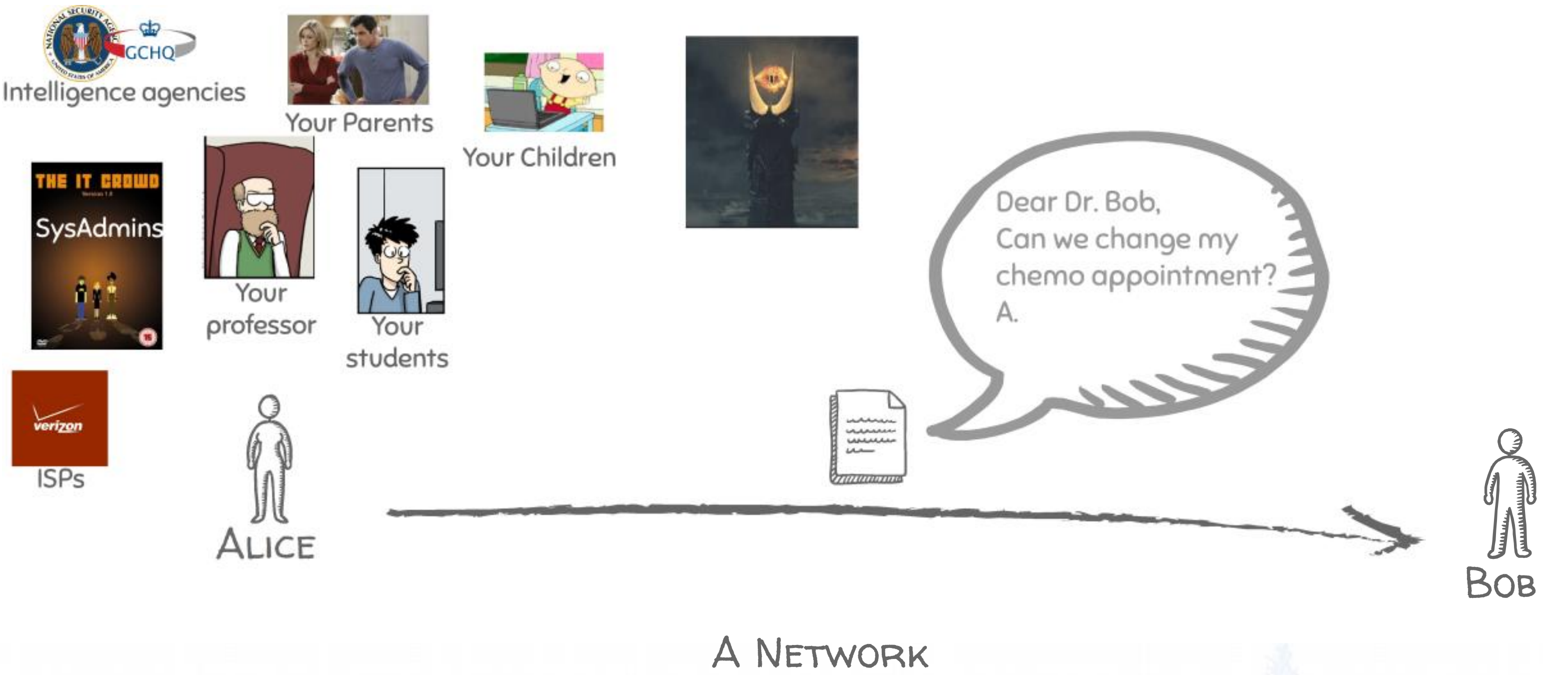
Alice

Dear Dr. Bob,
Can we change my chemo appointment?
A.

Bob

A Network

Privacy in electronic communications



Intelligence agencies

Your Parents

Your Children

SysAdmins

Your professor

Your students

ISPs

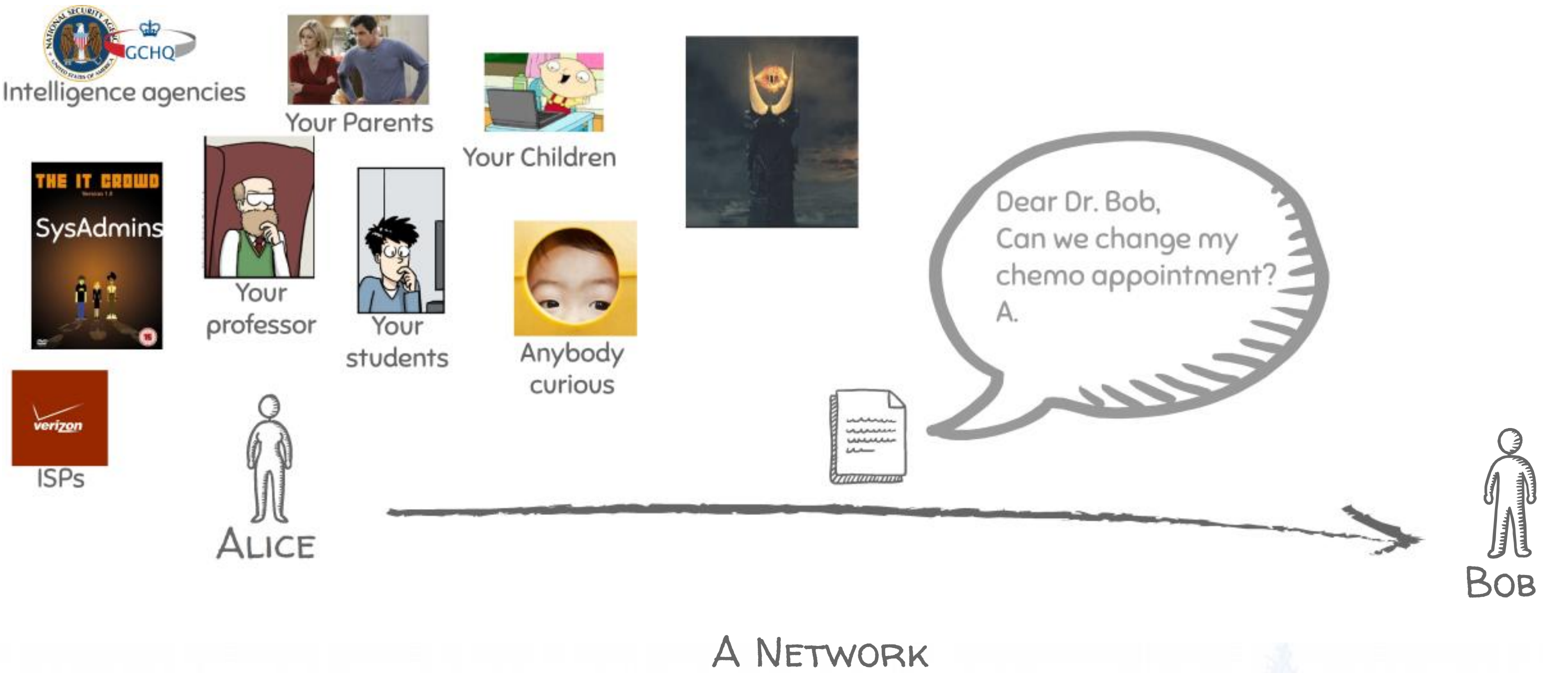
Dear Dr. Bob,
Can we change my
chemo appointment?
A.

Alice

Bob

A Network

Privacy in electronic communications



Intelligence agencies

Your Parents

Your Children

SysAdmins

Your professor

Your students

Anybody curious

ISPs

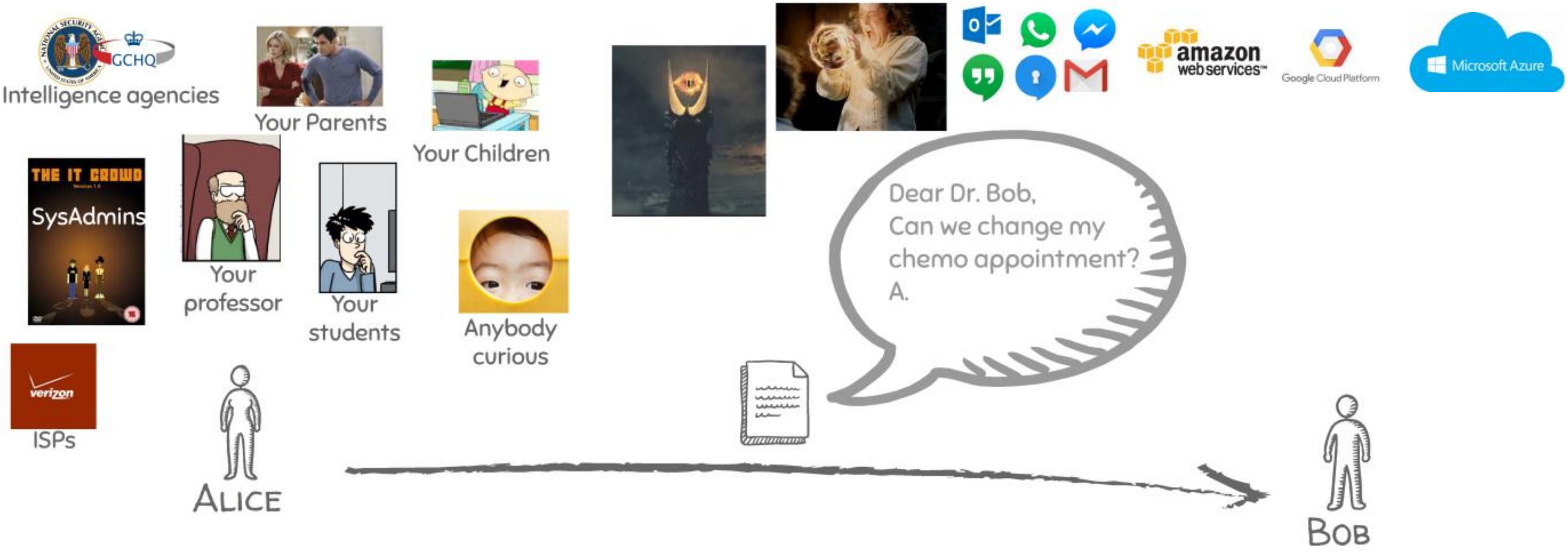
Dear Dr. Bob,
Can we change my chemo appointment?
A.

Alice

Bob

A Network

Privacy in electronic communications



Intelligence agencies

Your Parents

Your Children

SysAdmins

Your professor

Your students

Anybody curious

ISPs

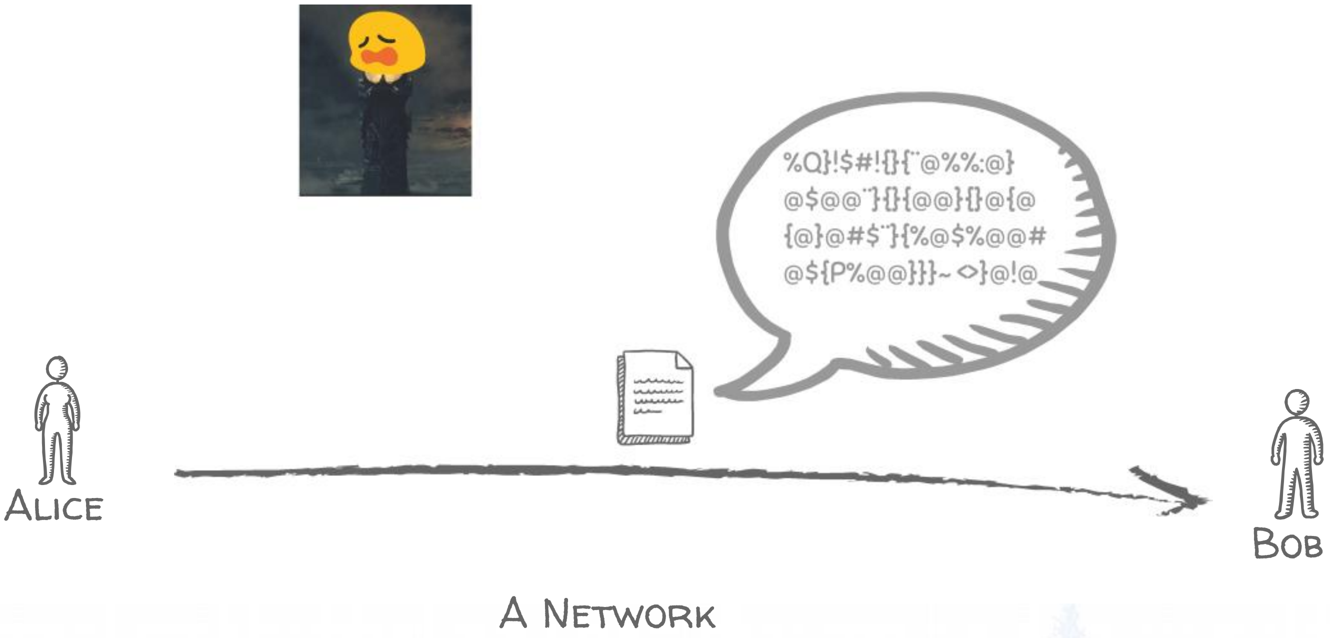
Alice

Dear Dr. Bob,
Can we change my chemo appointment?
A.

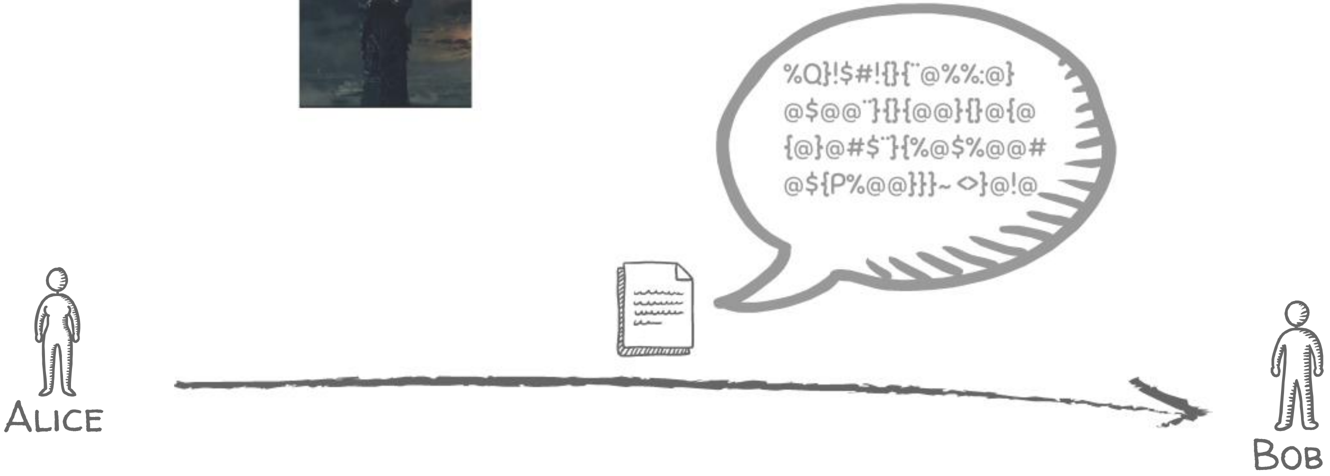
Bob

A Network

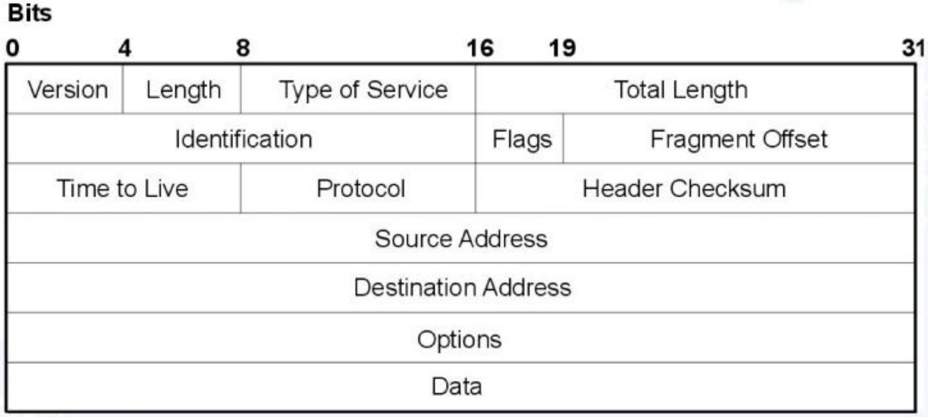
But we can encrypt! What is the problem?



But we can encrypt! What is the problem?



A Network



Bits

0 4 8 16 19 31

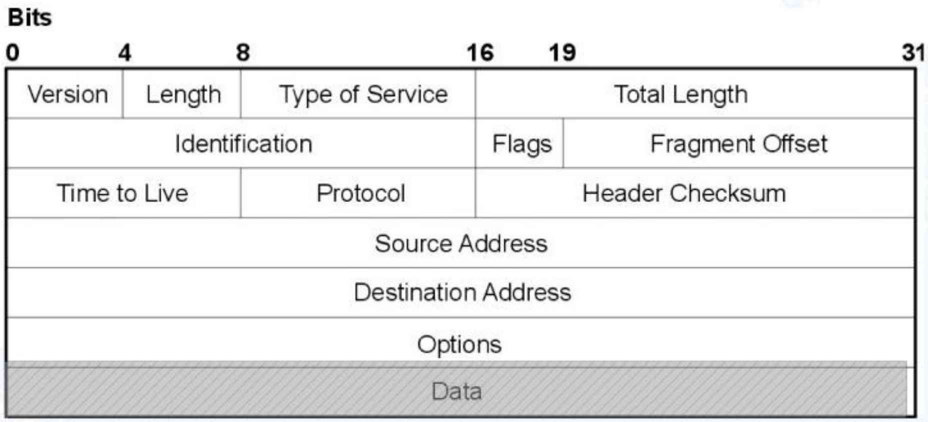
Version	Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				
Data				

IPv4 Header
(RFC 791, 1981)

But we can encrypt! What is the problem?

%Q}!$#!{}{¨@%%:@}
@$@@¨}{}{@@}{}@{@
{@}@#$¨}{%@$%@@#
@${P%@@}}}~<>}@!@
Alice
Bob

A Network



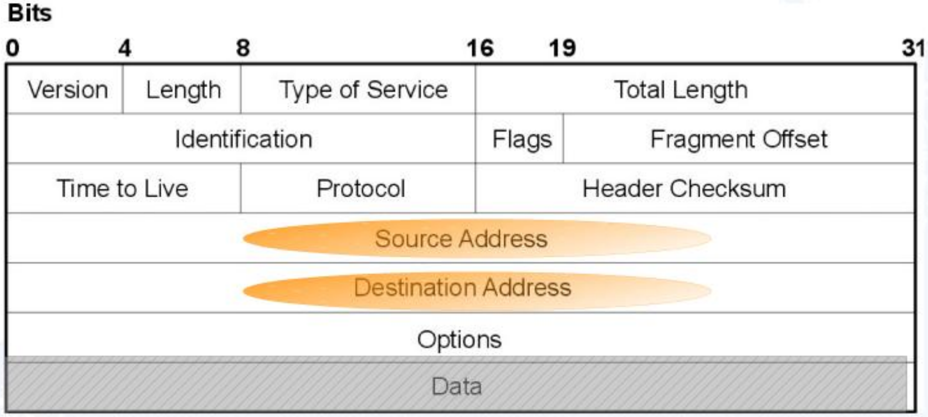
Bits

0	4	8	16	19 31
Version	Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				
Data				

IPv4 Header
(RFC 791, 1981)

But we can encrypt! What is the problem?

%Q}!$#!{}{¨@%%:@}
@$@@¨}{}{@@}{}@{@
{@}@#$¨}{%@$%@@#
@${P%@@}}}~<>}@!@
Alice
Bob
A Network

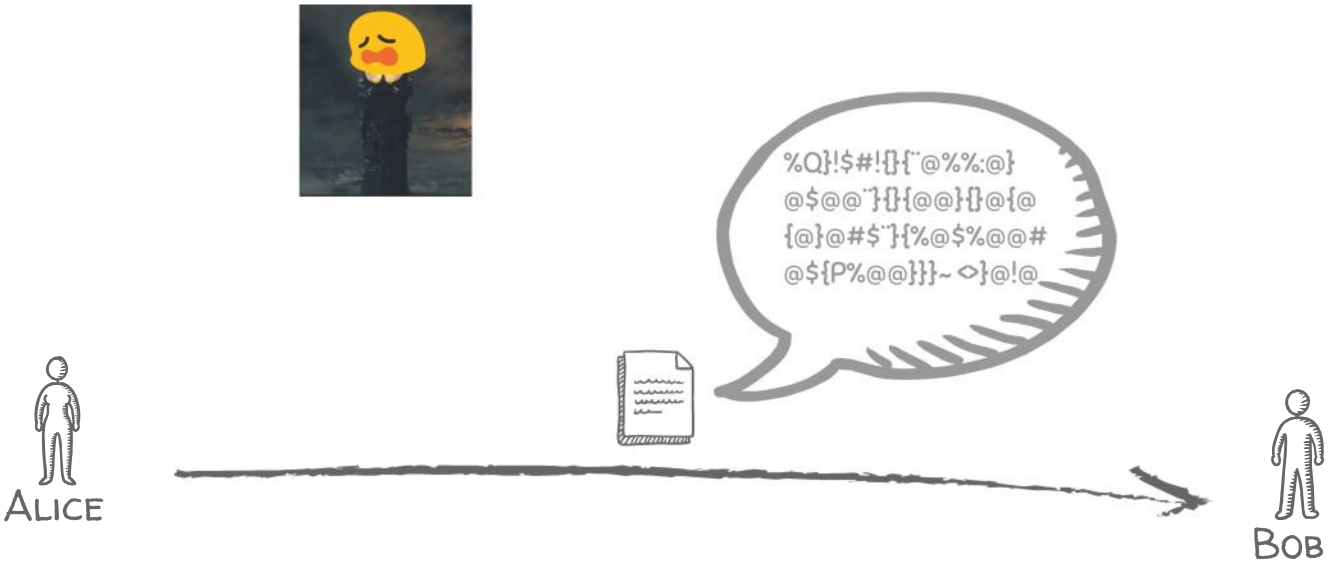


Bits

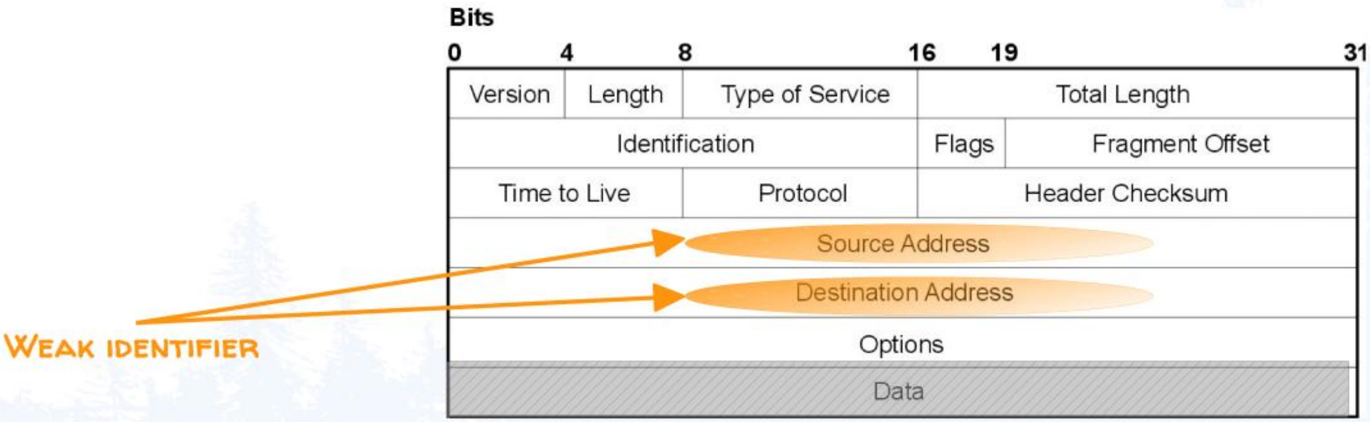
0	4	8	16	19	31
Version	Length	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol	Header Checksum		
Source Address					
Destination Address					
Options					
Data					

IPv4 Header
(RFC 791, 1981)

But we can encrypt! What is the problem?



A Network

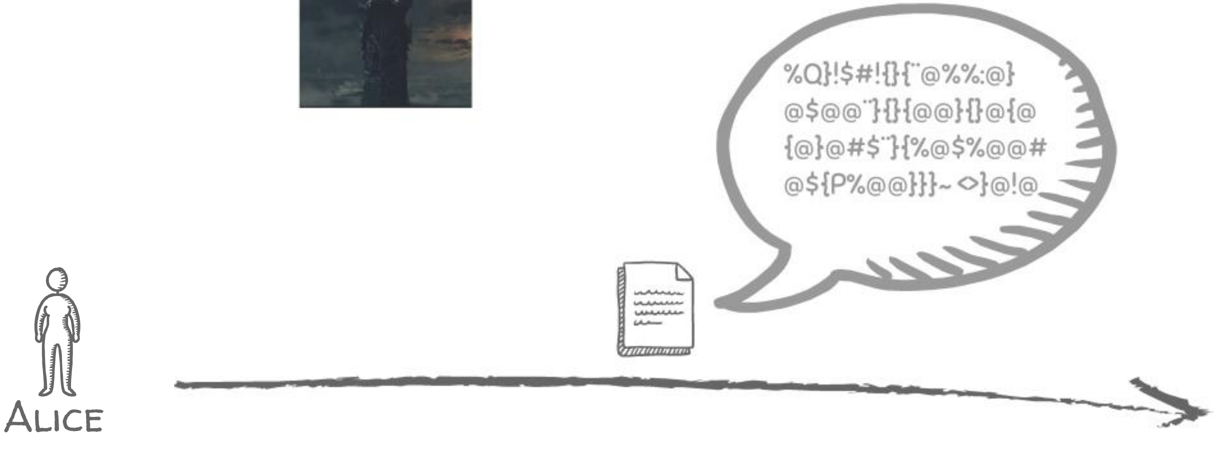


Bits

0–3	4–7	8–15	16–18	19–31
Version	Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				
Data				

IPv4 Header
(RFC 791, 1981)

But we can encrypt! What is the problem?



A Network

Bits

0 4 8 16 19 31

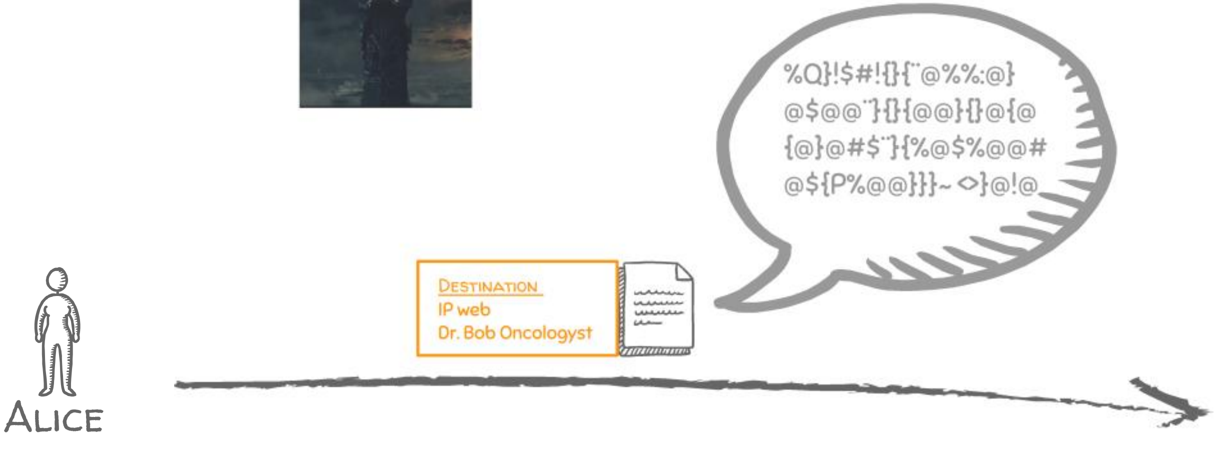
<table>
<tr><td>Version</td><td>Length</td><td>Type of Service</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Options</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Weak identifier

IPv4 Header
(RFC 791, 1981)

Same for Ethernet, TCP, SMTP, IRC, HTTP, ...

But we can encrypt! What is the problem?



A Network

Bits

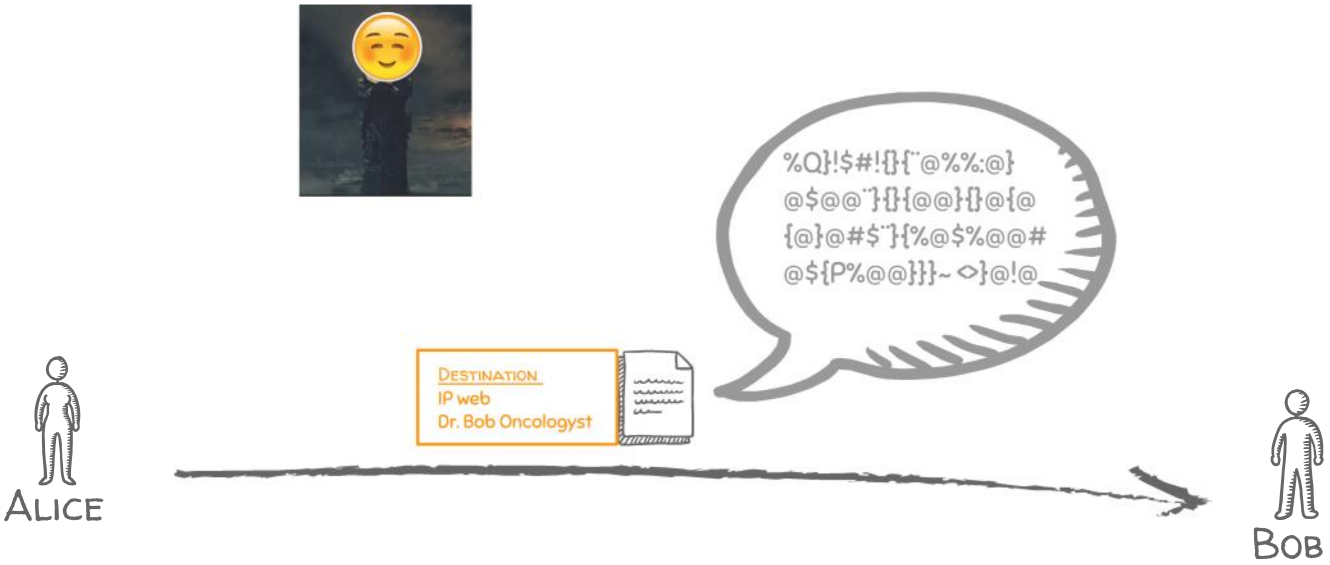
0	4	8	16	19	31
Version	Length	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol	Header Checksum		
Source Address					
Destination Address					
Options					
Data					

Weak identifier

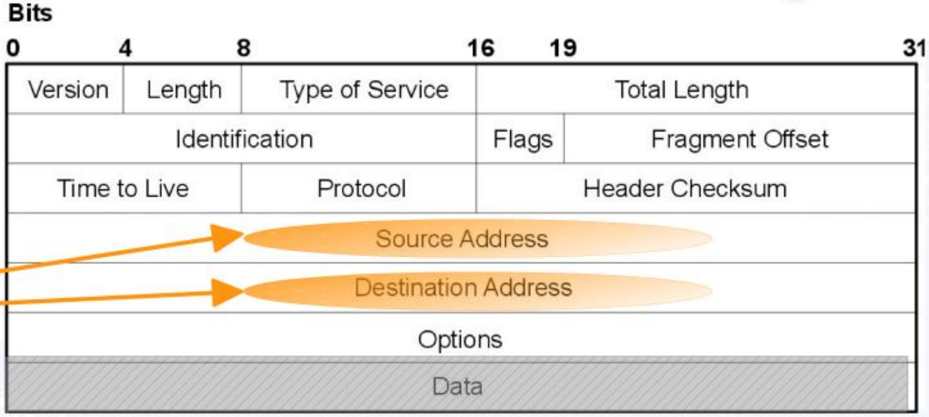
IPv4 Header
(RFC 791, 1981)

Same for Ethernet, TCP, SMTP, IRC, HTTP, ...

The problem is Traffic Analysis!!



A Network



Bits

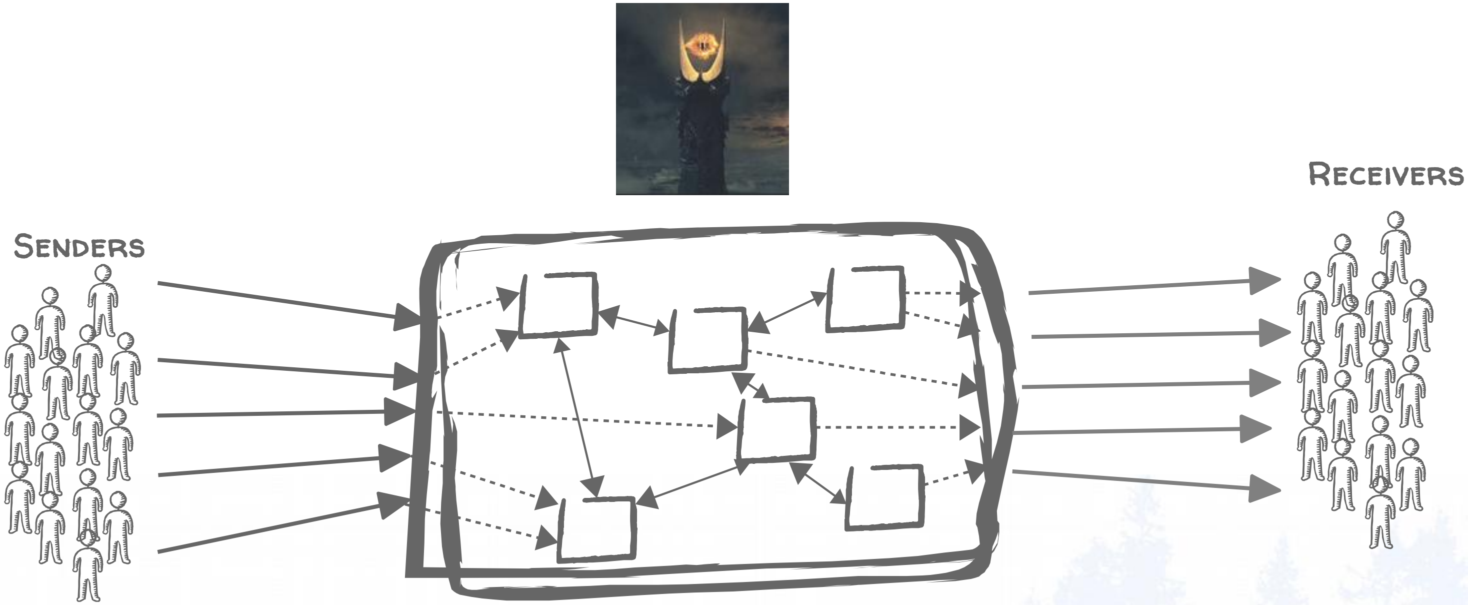
0	4	8	16	19	31
Version	Length	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live		Protocol	Header Checksum		
Source Address					
Destination Address					
Options					
Data					

Weak identifier

IPv4 Header
(RFC 791, 1981)

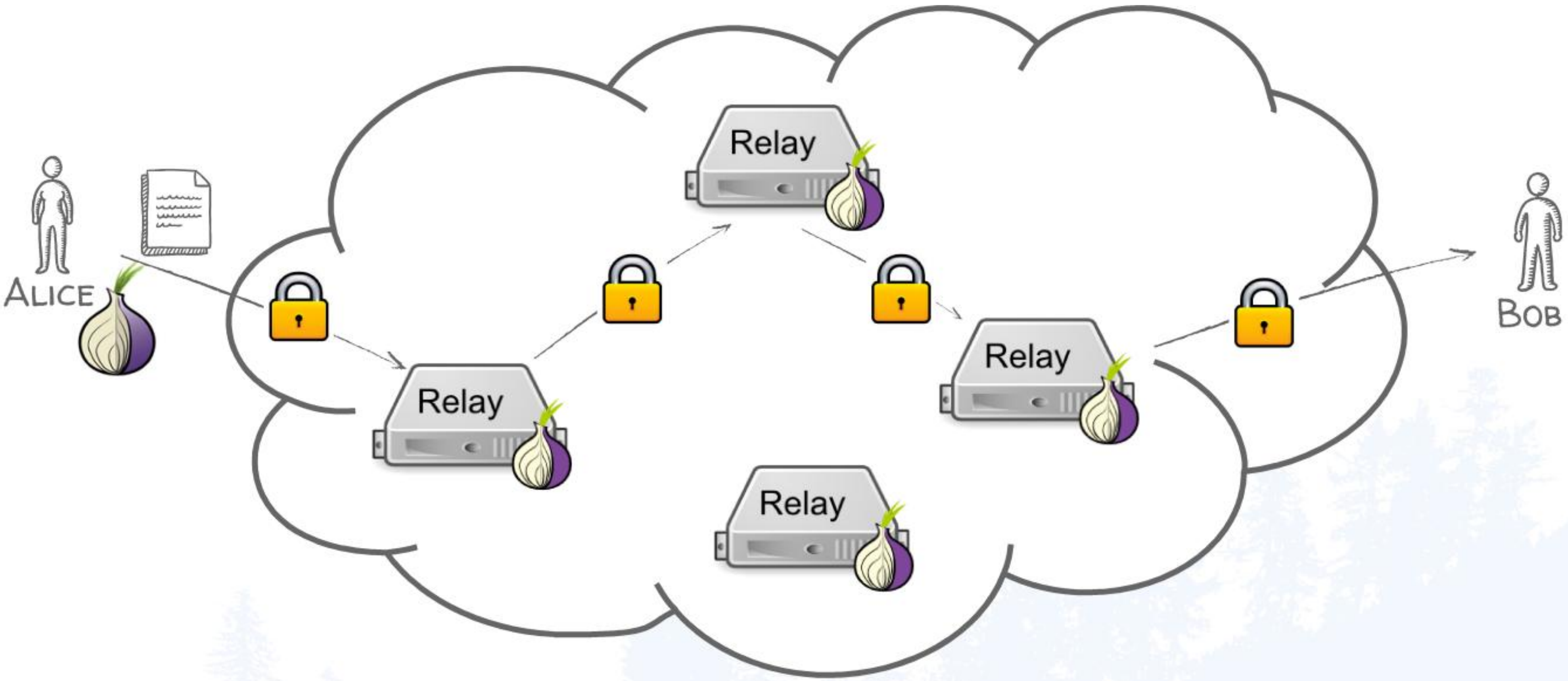
Same for Ethernet, TCP, SMTP, IRC, HTTP, ...

Traffic analysis resistance: Anonymous communications

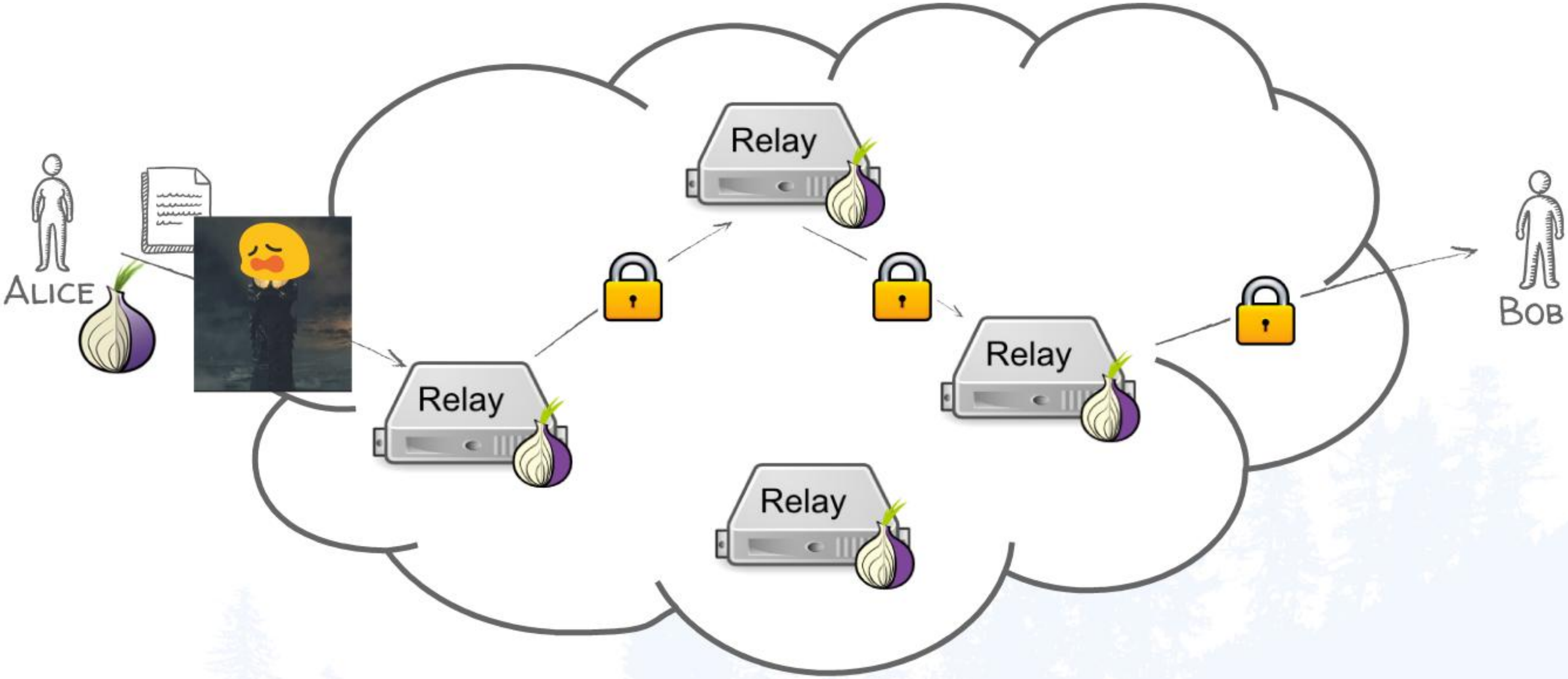


- Bitwise unlinkability
  - Crypto to make inputs and outputs bit patterns different
- (re)packetizing + (re)schedule + (re)routing,
  - Destroy patterns (traffic analysis resistance)
  - Load balancing
  - Distribute trust

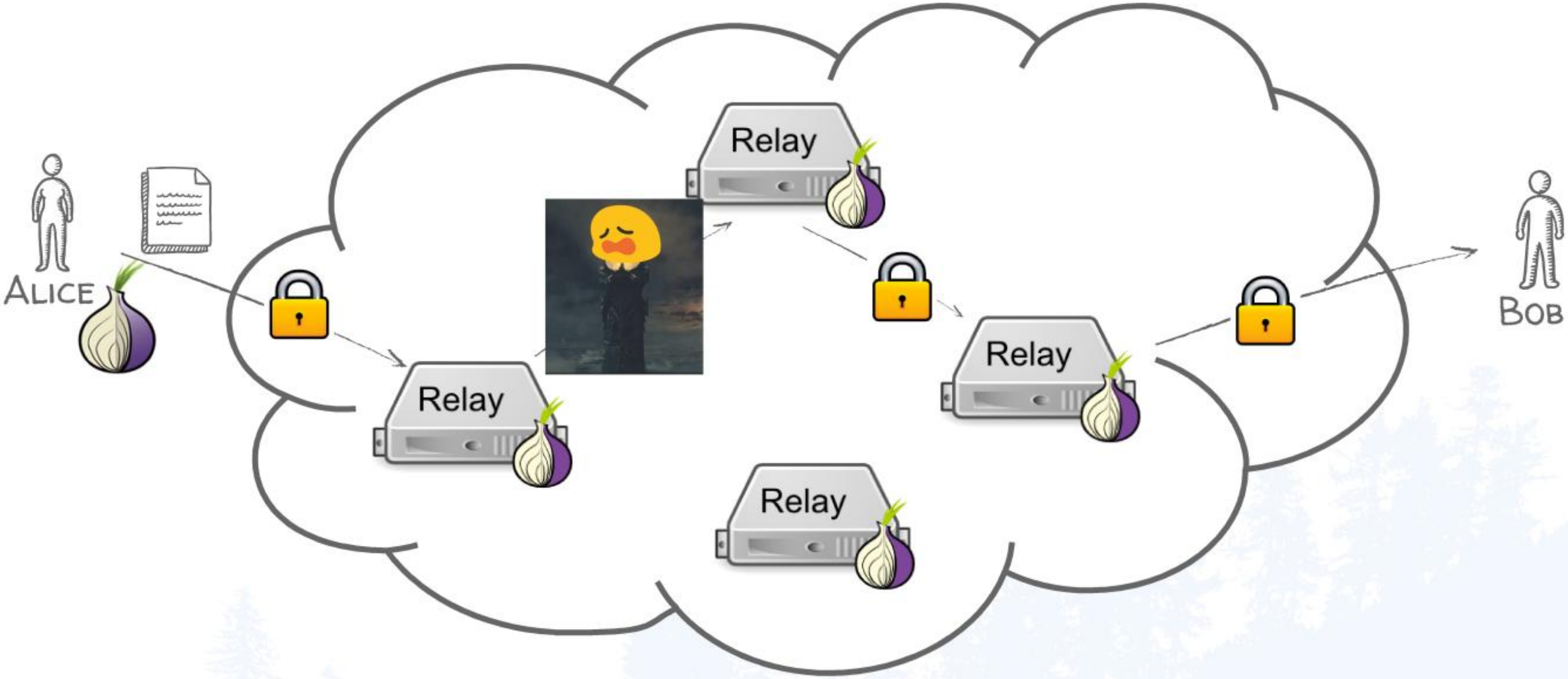
The Tor Network



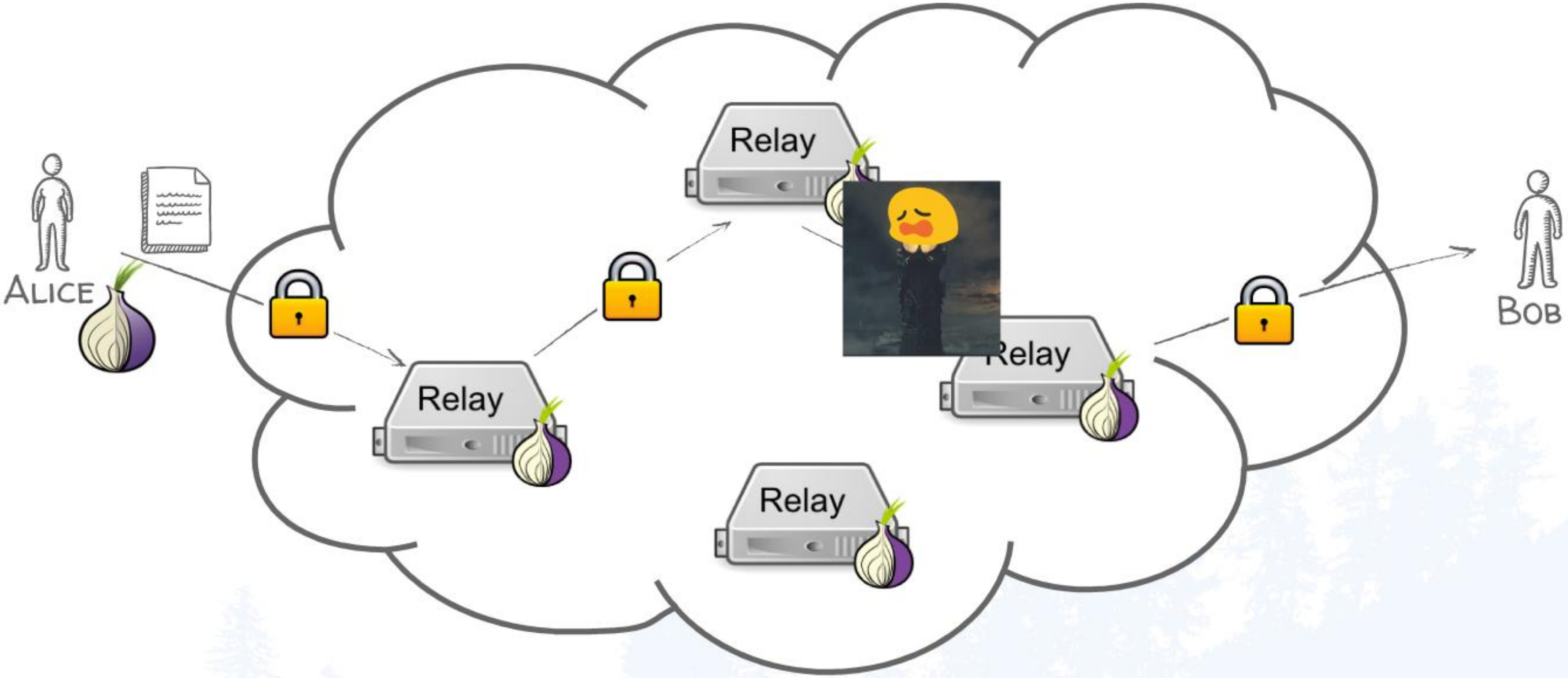
The Tor Network



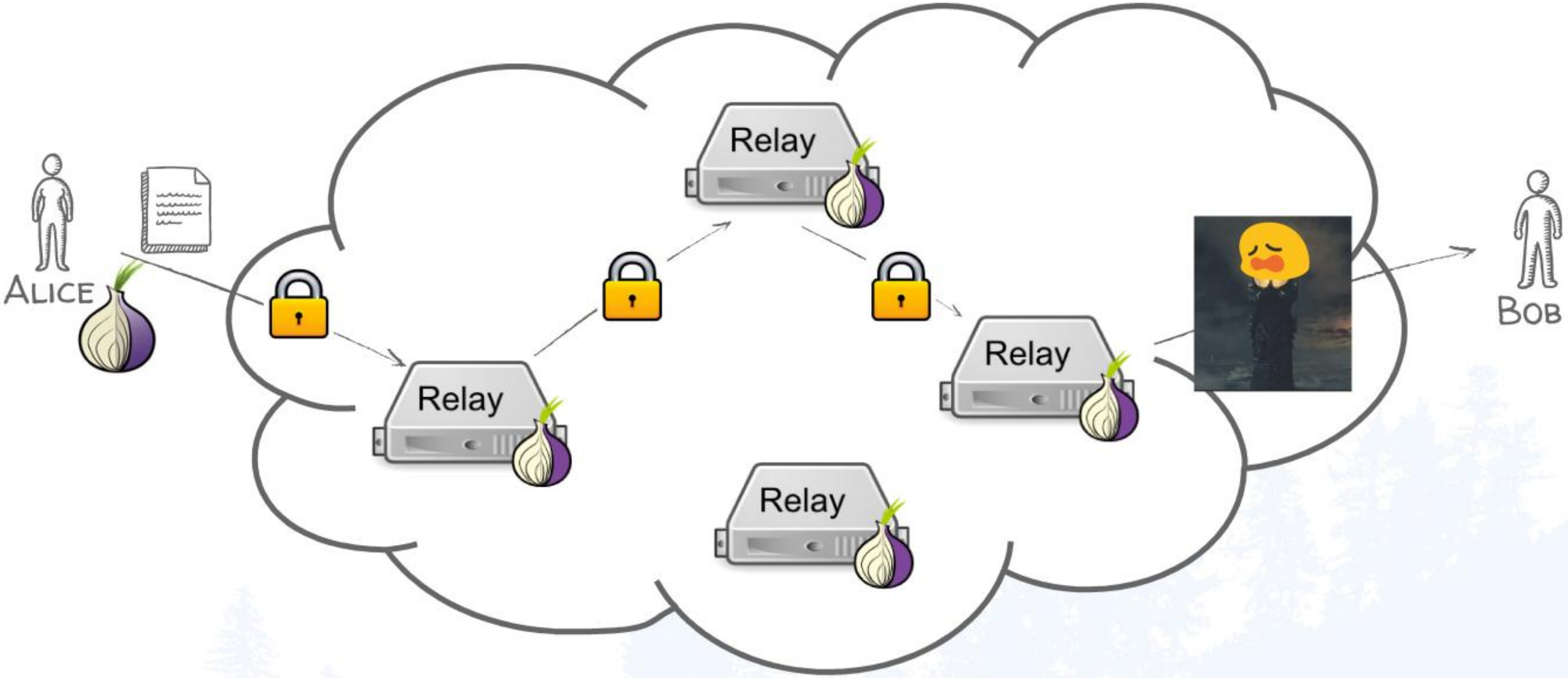
The Tor Network



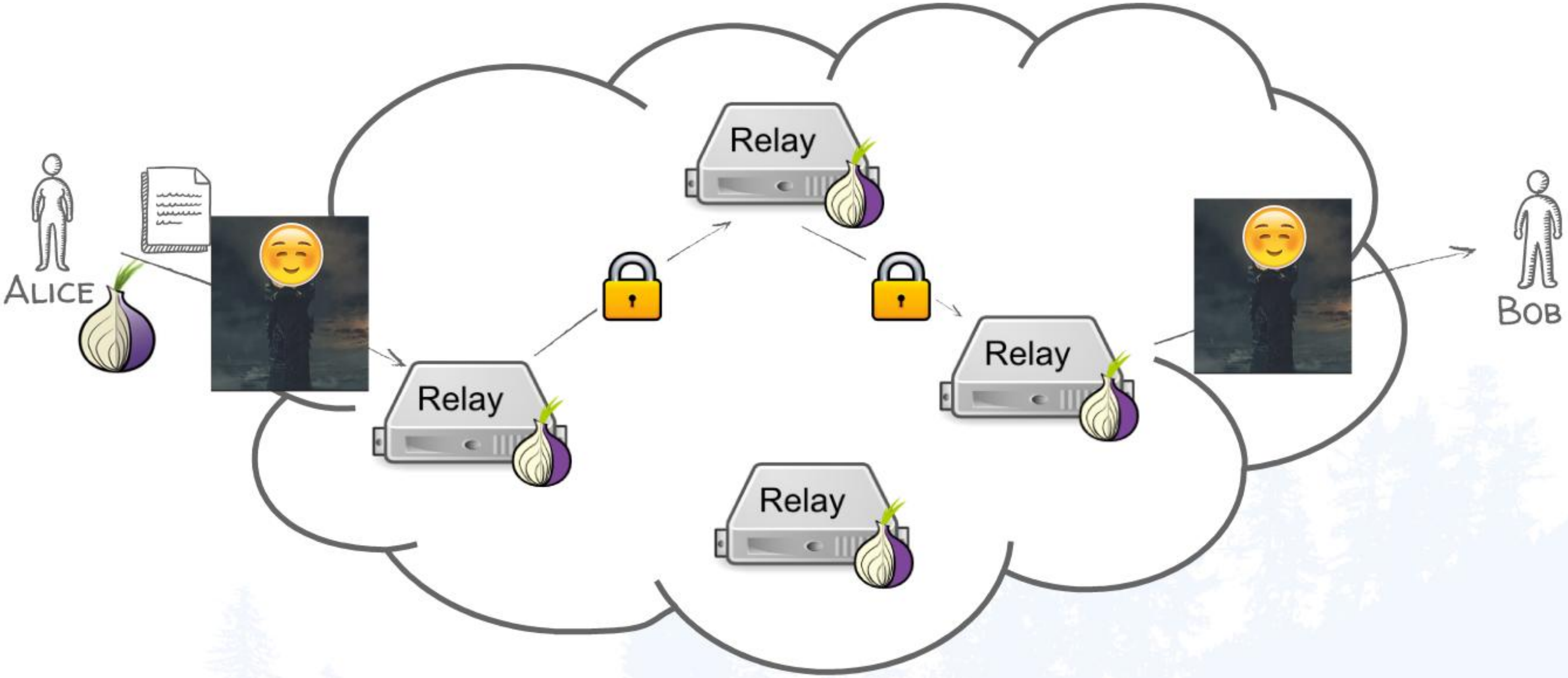
The Tor Network



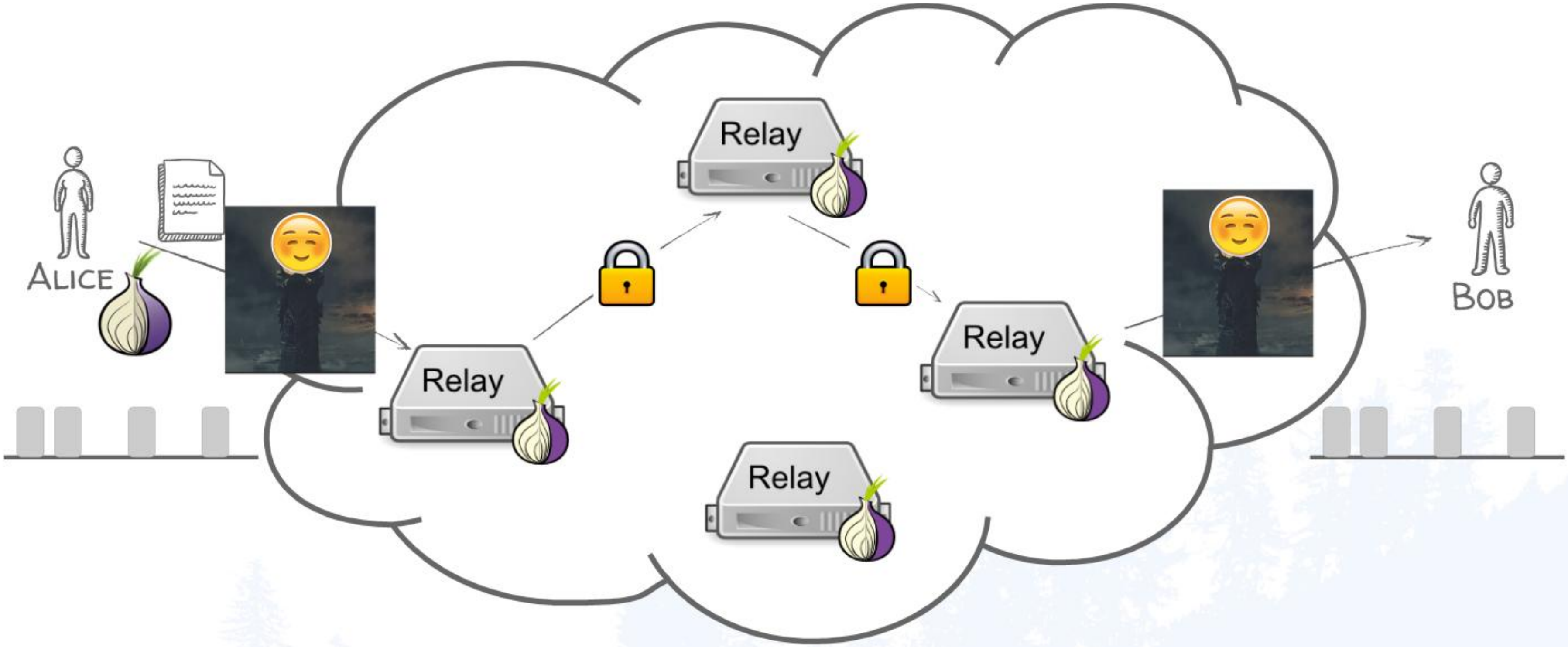
The Tor Network



The Tor Network

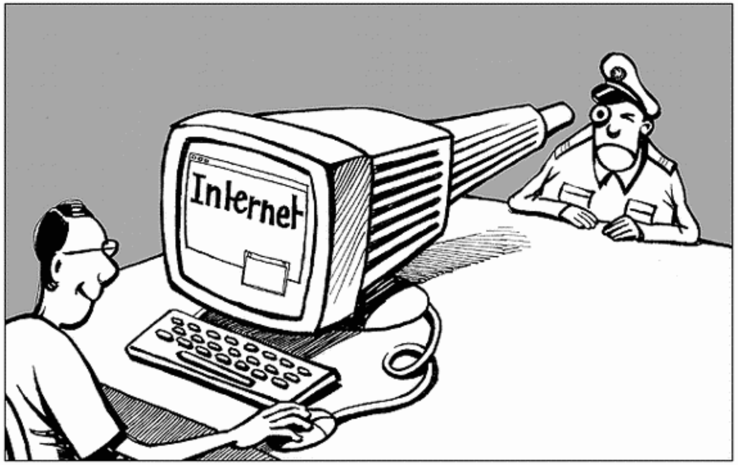


The Tor Network

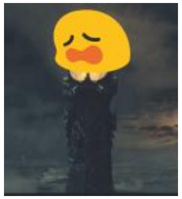


Low latency = High correlation!

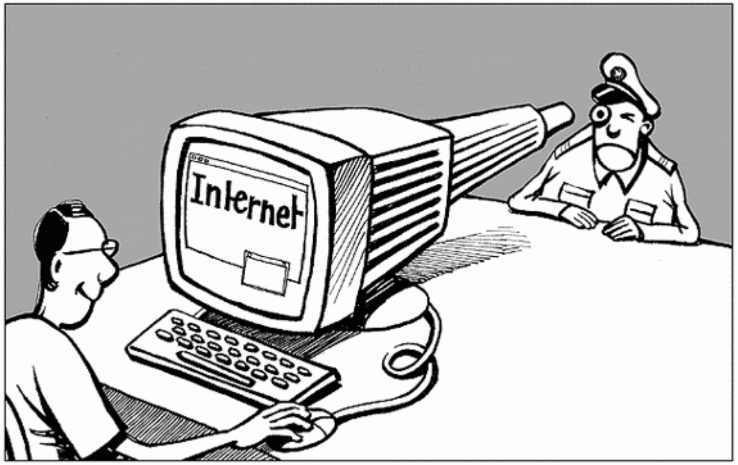
The Tor Network – Goals



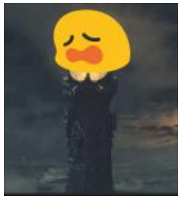
Surveillance and monitoring protection

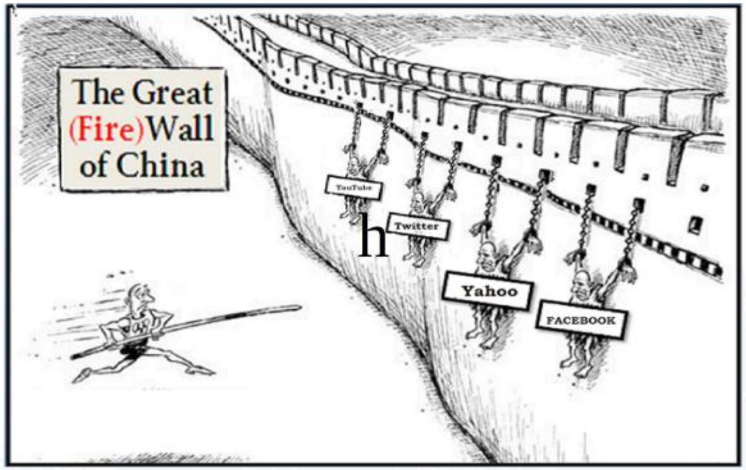


The Tor Network – Goals



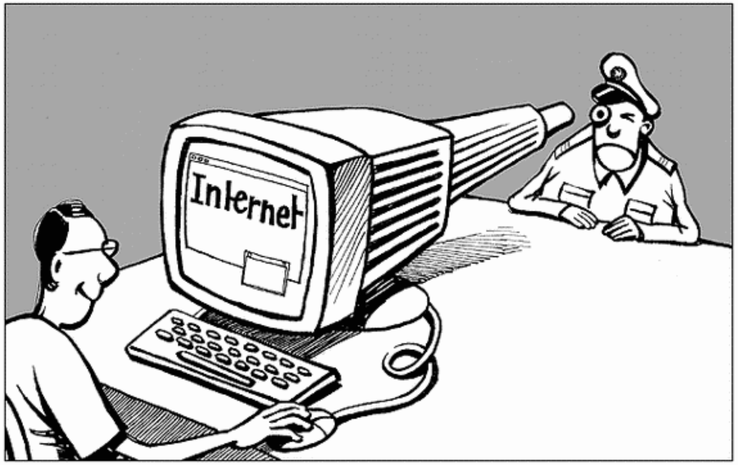
Surveillance and monitoring protection



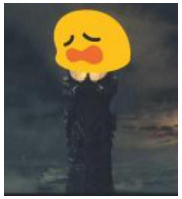


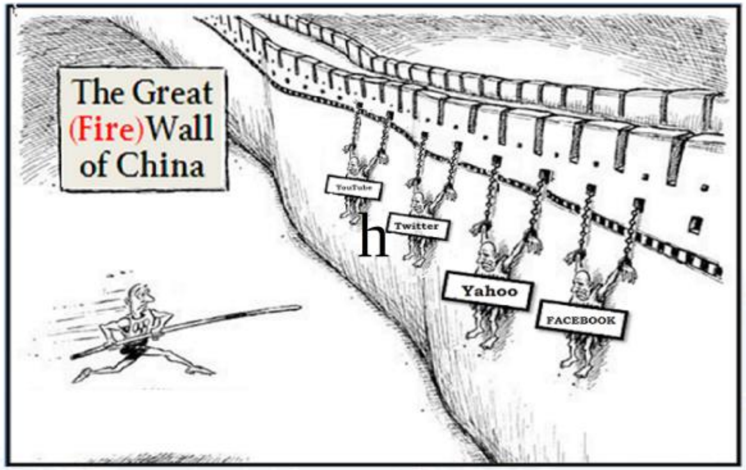
Censorship circumvention

The Tor Network – Goals



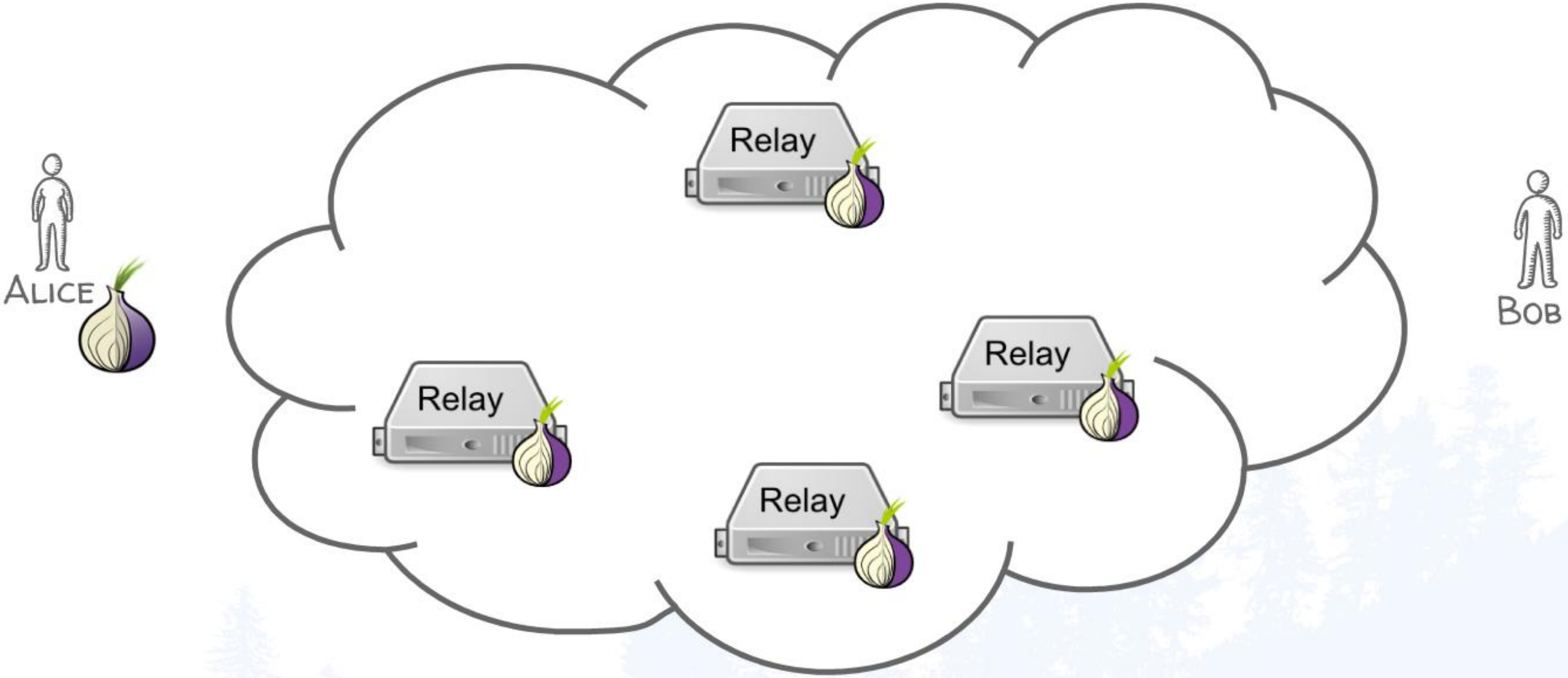
Surveillance and monitoring protection





Censorship circumvention

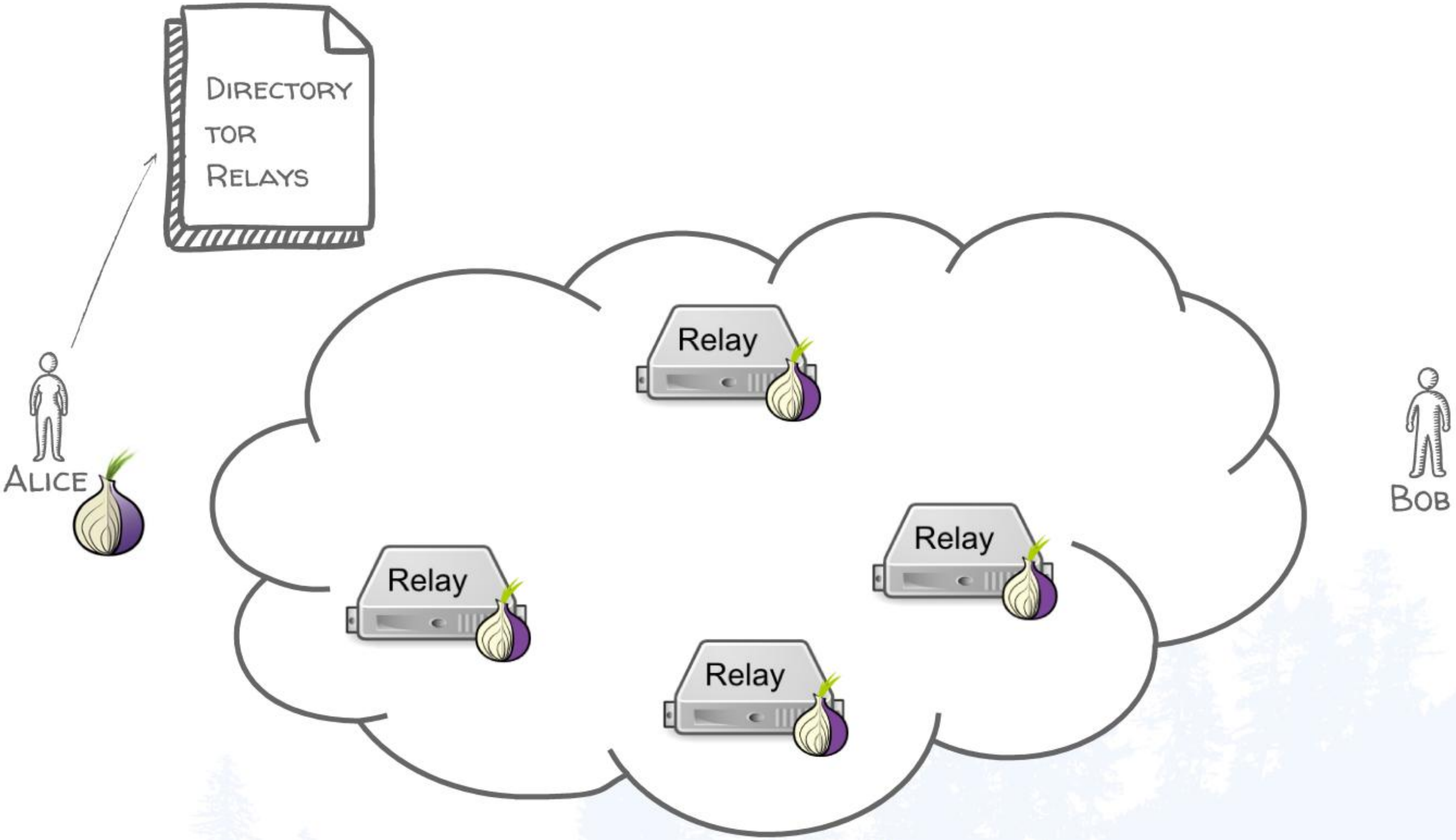
But can Block Tor!



The Tor Network

TorProject.org

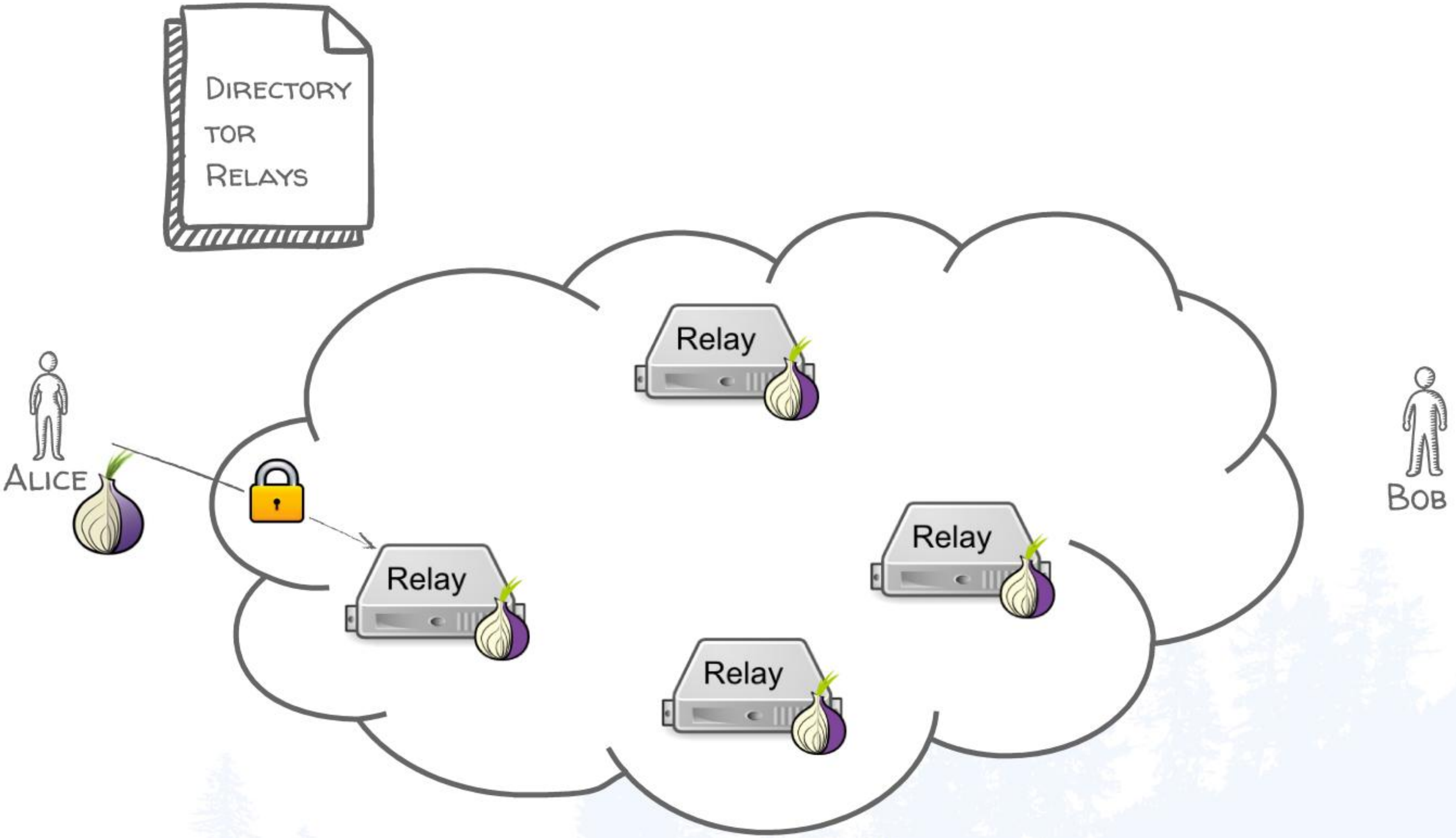
But can Block Tor!



The Tor Network

TorProject.org

But can Block Tor!

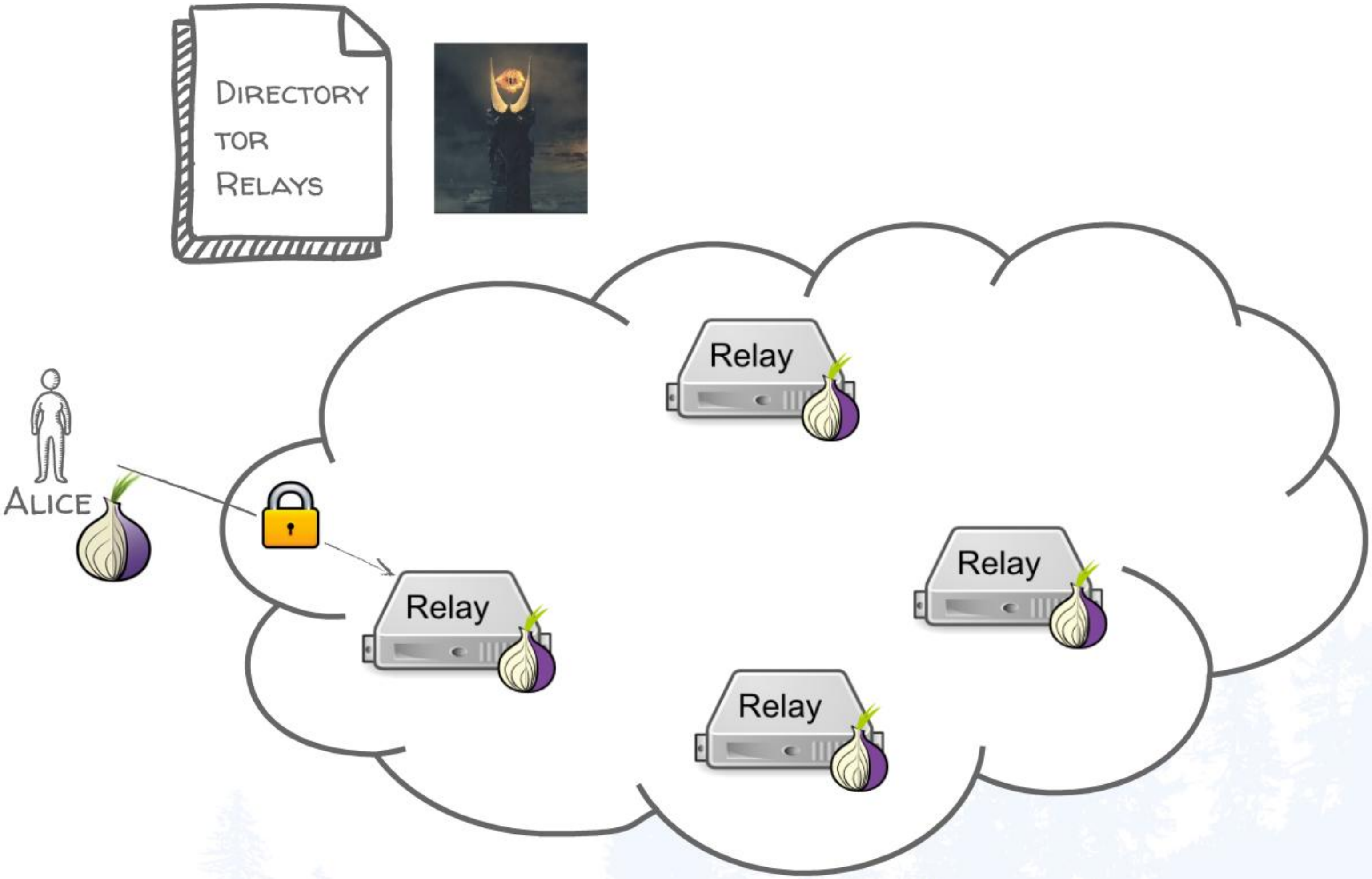


The Tor Network

Tor®

TorProject.org

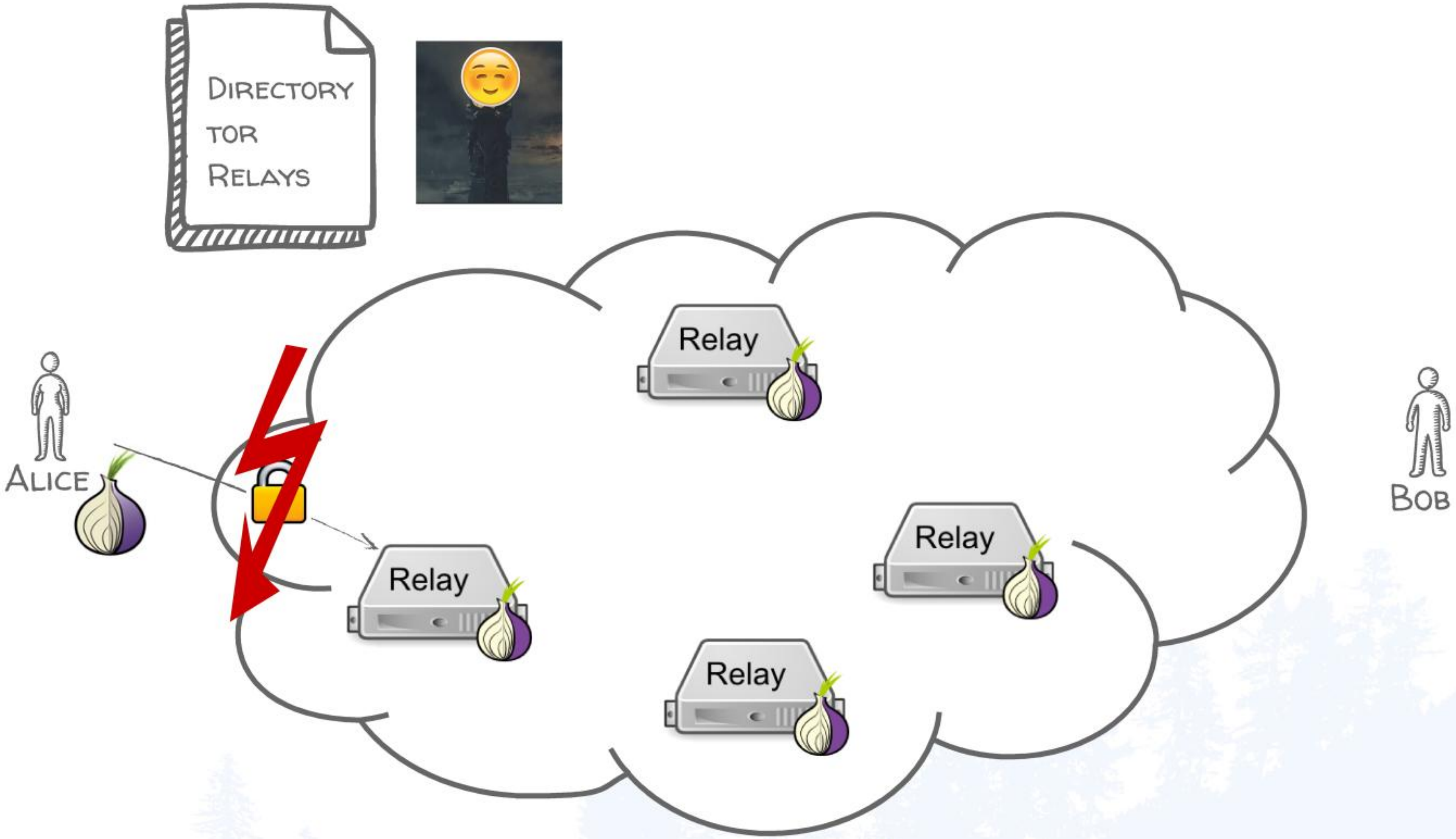
But can Block Tor!



The Tor Network

TorProject.org

But can Block Tor!

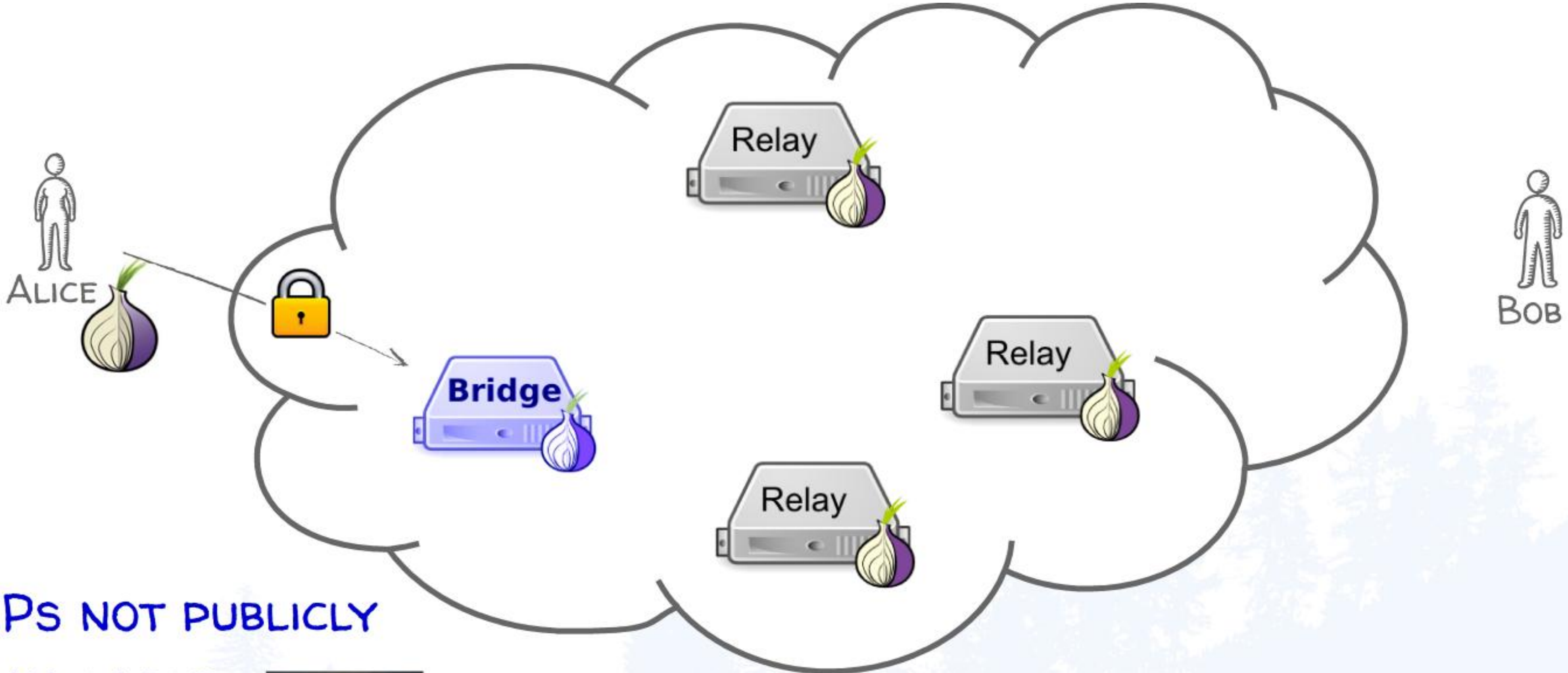


The Tor Network

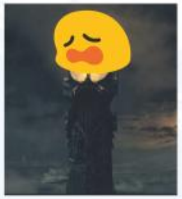
Tor®

TorProject.org

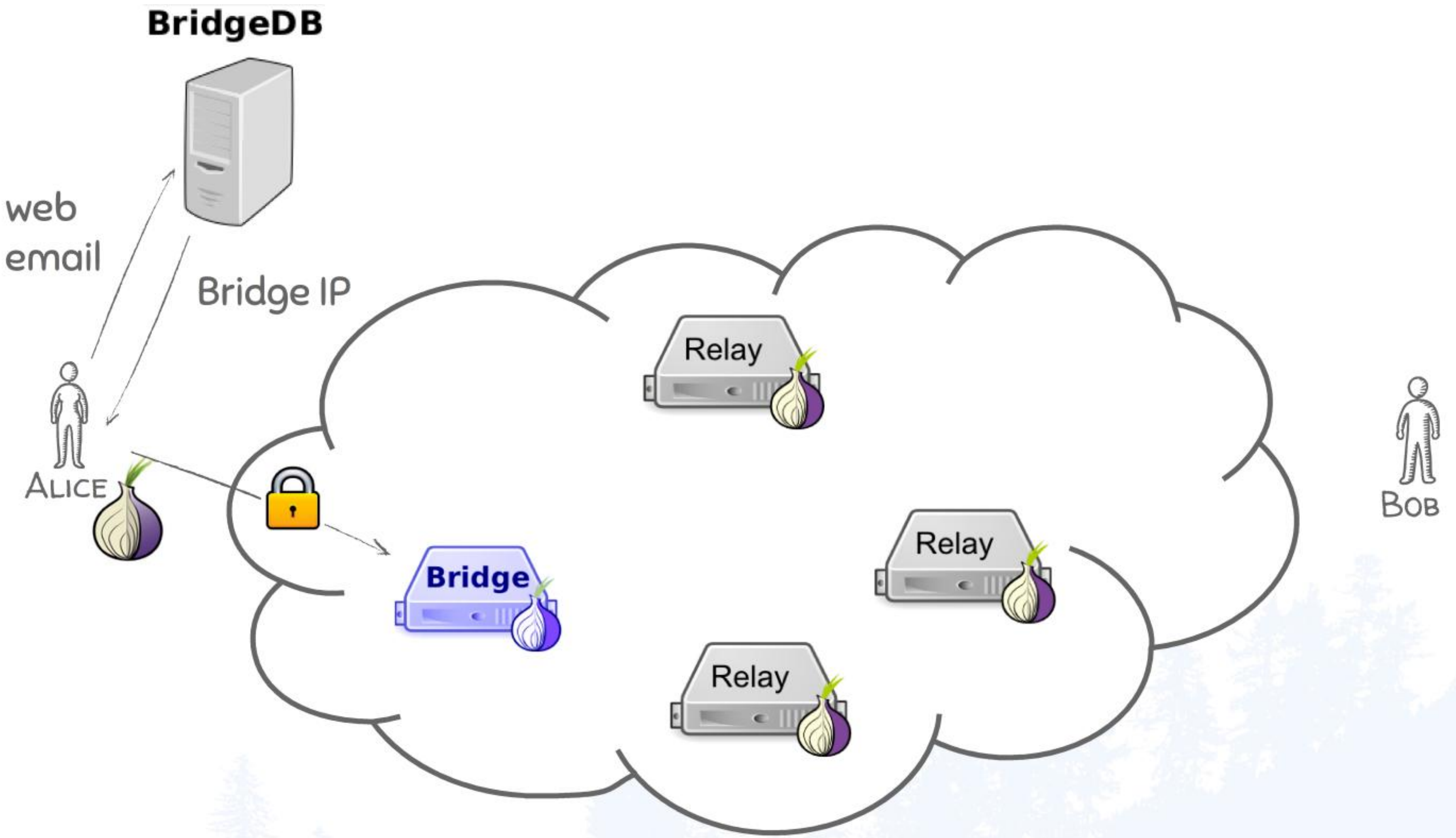
Censorship circumvention – Bridges



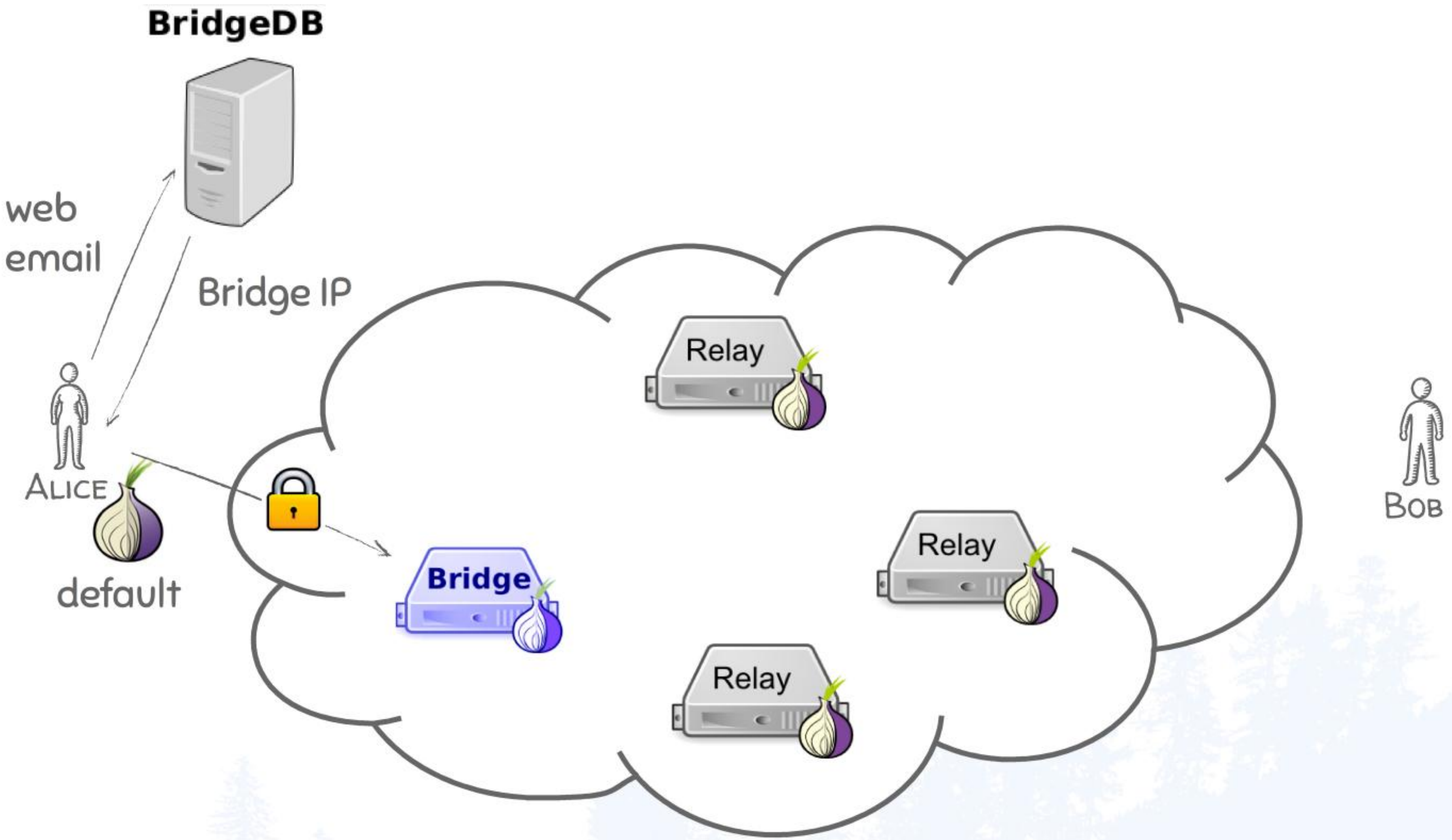
IPs not publicly available



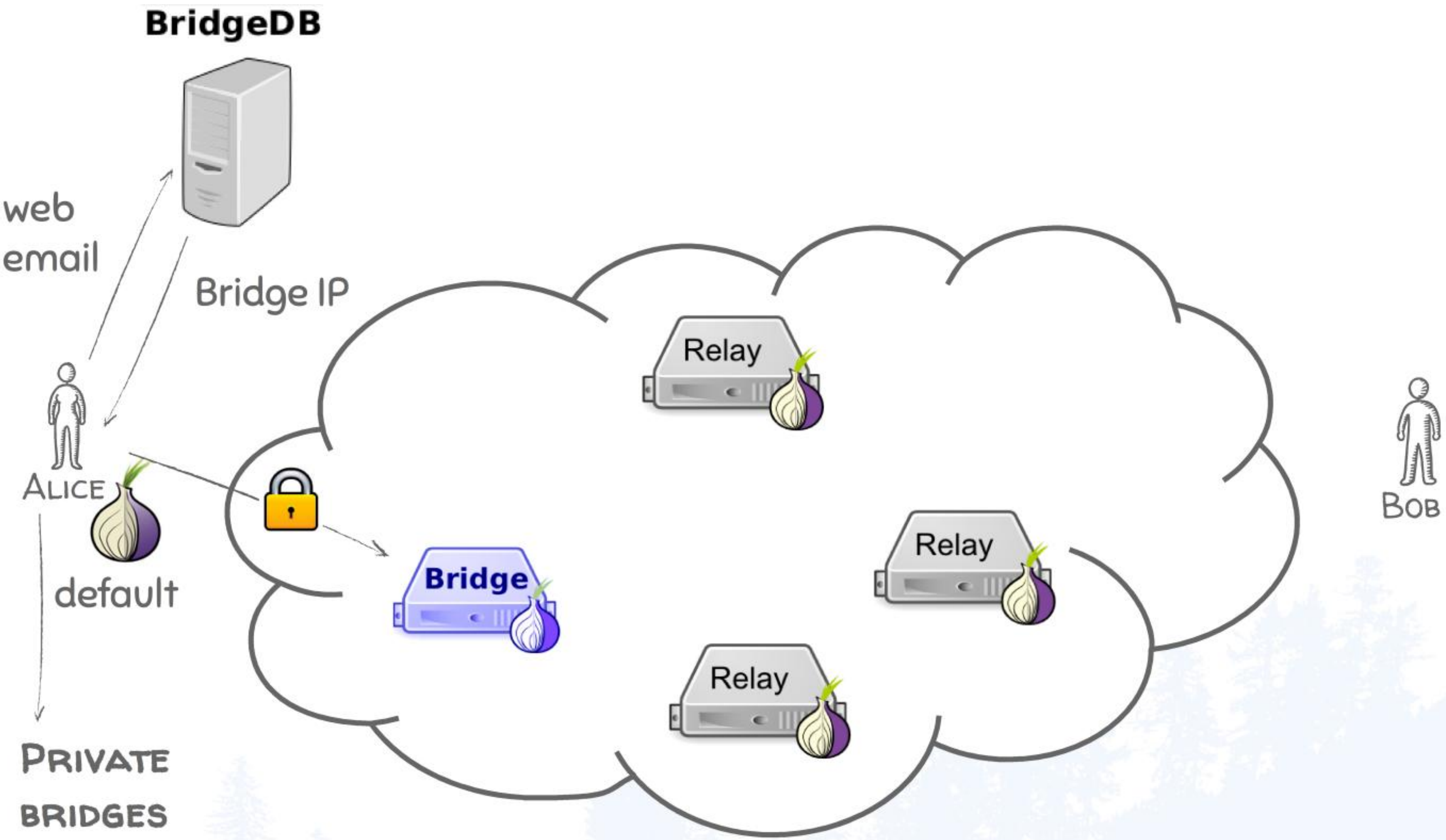
Censorship circumvention – finding Bridges



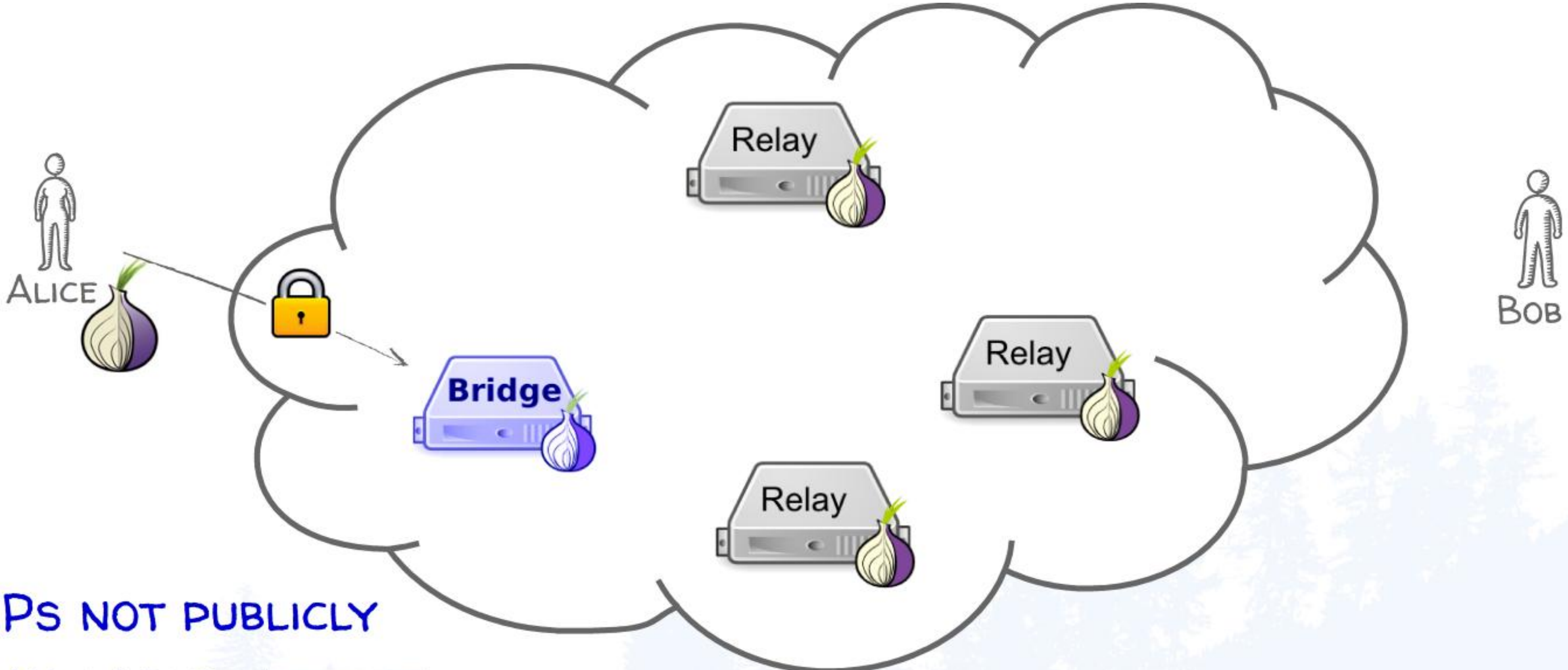
Censorship circumvention – finding Bridges



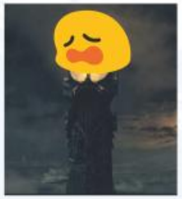
Censorship circumvention – finding Bridges



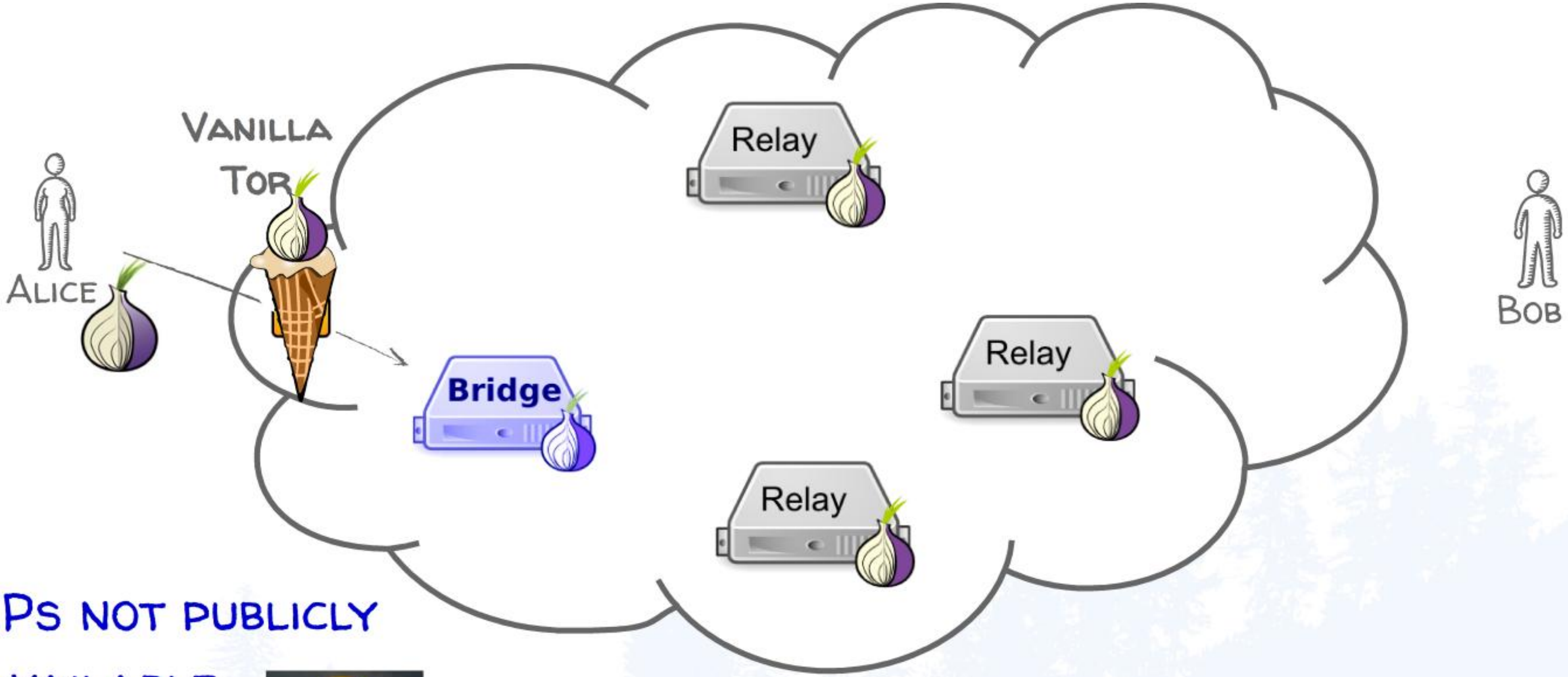
What about Traffic analysis?



IPs not publicly available

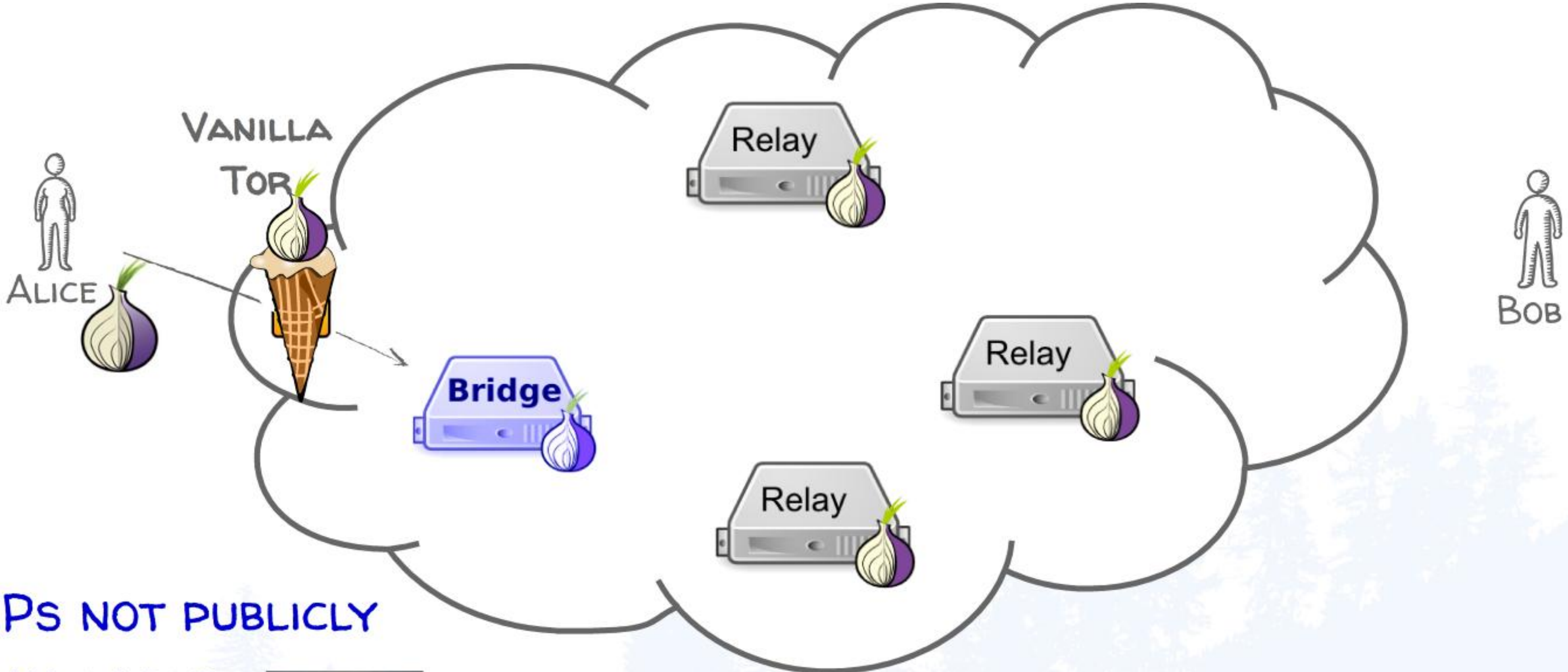


What about Traffic analysis?



IPs not publicly available

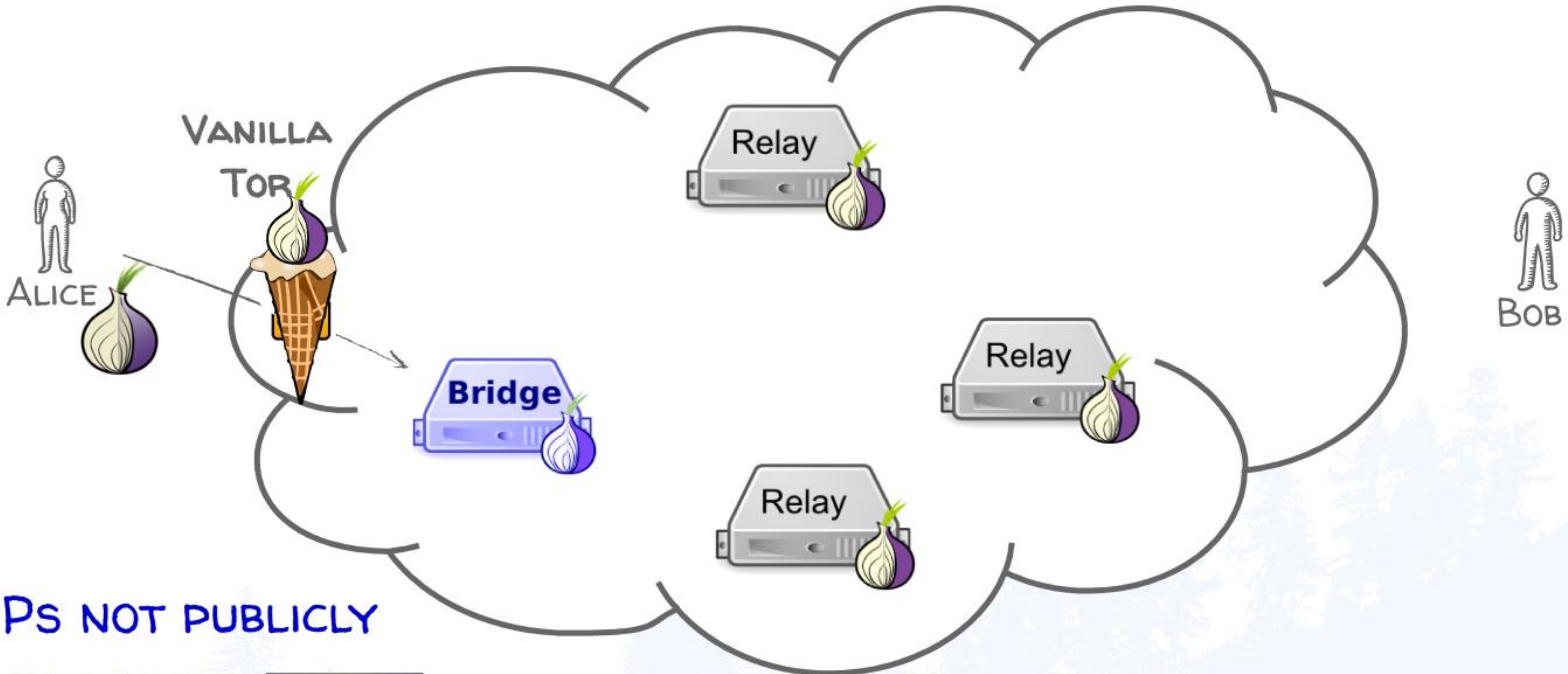
What about Traffic analysis?



IPs not publicly available

Vanilla Tor recognizable!

What about Traffic analysis?

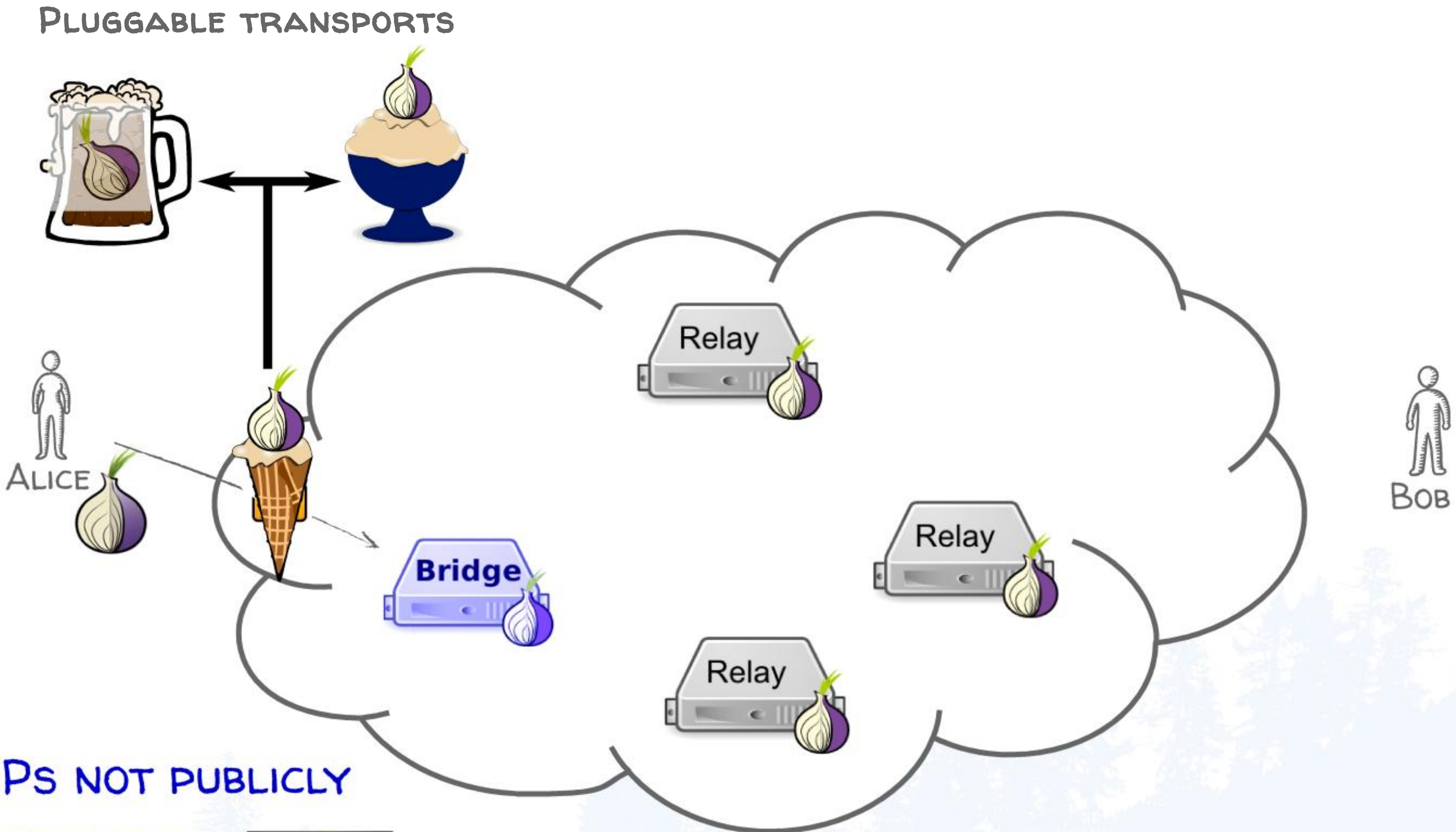


IPs not publicly available

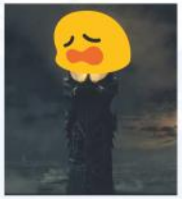
Vanilla Tor recognizable!

←Traffic Analysis!!

What about Traffic analysis?



IPs not publicly available



Pluggable Transports **not** Recognizable

Studying Bridges

❶ Onion Router whose IP is not publicly listed
❷ is always elected as the first hop
❸ can offer multiple Pluggable Transports.

Studying Bridges – Our goals

❶ Onion Router whose IP is not publicly listed
❷ is always elected as the first hop
❸ can offer multiple Pluggable Transports.

Perform first systematic study of the security of the Tor bridge infrastructure

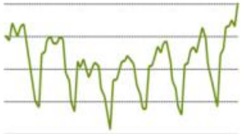
Studying Bridges – Our goals

❶ Onion Router whose IP is not publicly listed
❷ is always elected as the first hop
❸ can offer multiple Pluggable Transports.

Perform first systematic study of the security of the Tor bridge infrastructure

Public bridges

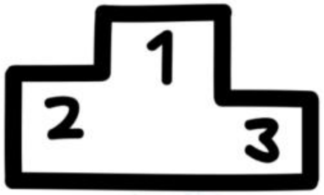
population



stability

PT deployment

OR port distribution



Ranking

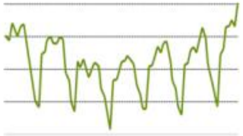
Studying Bridges – Our goals

❶ Onion Router whose IP is not publicly listed
❷ is always elected as the first hop
❸ can offer multiple Pluggable Transports.

Perform first systematic study of the security of the Tor bridge infrastructure

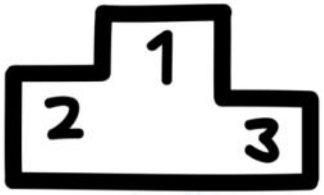
Public bridges

population


stability

PT deployment

OR port distribution



Ranking

Private bridges

population

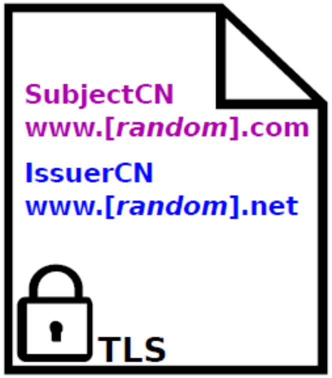
clustering

proxys!

We exploit…

Two issues known to Tor project since October 2010

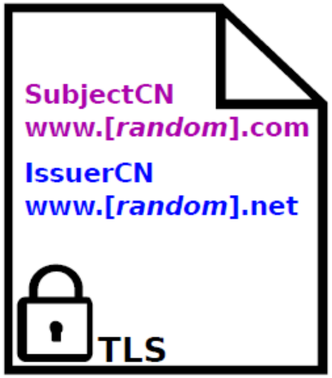
1. Vanilla Tor Certificates
   - Vanilla Tor uses TLS handshake
   - Easy to spot certificates
   - It won't be fixed



We exploit...

Two issues known to Tor project since October 2010

1. Vanilla Tor Certificates
   - Vanilla Tor uses TLS handshake
   - Easy to spot certificates
   - It won't be fixed



SubjectCN
www.[*random*].com

IssuerCN
www.[*random*].net

TLS

2. Open OR Port
   - Bridges have open OR Port with Vanilla Tor
   - Even if they do not offer Vanilla Tor
   - Difficult to fix

We exploit...

Two is ... **er 2010**

1.

2.

We exploit...

Two is … er 2010

1.

2.

We use three datasets

SHODAN

Scan 200+ ports with multiple protocols
19 ports scanned with TLS
Indexed data available

censys

Scan 6 ports with TLS
Raw + indexed data available

We use three datasets

SHODAN

Scan 200+ ports with multiple protocols
19 ports scanned with TLS
Indexed data available

censys

Scan 6 ports with TLS
Raw + indexed data available

Identify candidate bridge IPs
(without scanning ourselves!!)

We use three datasets

SHODAN

Scan 200+ ports with multiple protocols
19 ports scanned with TLS
Indexed data available

censys

Scan 6 ports with TLS
Raw + indexed data available

Identify candidate bridge IPs
(without scanning ourselves!!)

COLLECTor

Node-level data on public bridges + relays
Some bridge data sanitized

We use three datasets

SHODAN

Scan 200+ ports with multiple protocols
19 ports scanned with TLS
Indexed data available

censys

Scan 6 ports with TLS
Raw + indexed data available

Identify candidate bridge IPs
(without scanning ourselves!!)

COLLECTor

Node-level data on public bridges + relays
Some bridge data sanitized

Is there sensitive data not anonymized?

Bridge discovery approach

Bridge discovery approach

1. Finding candidate IP addresses

censys

SHODAN

Bridge discovery approach

1. Finding candidate IP addresses
2. Filtering relays COLLECTor

censys

SHODAN

Bridge discovery approach

1. Finding candidate IP addresses
2. Filtering relays COLLECTor
3. Verifying IP addresses

censys

Shodan

Bridge discovery approach

1. Finding candidate IP addresses
2. Filtering relays
3. Verifying IP addresses
4. Identifying private proxies

   (check descriptor)

censys

SHODAN

COLLECTor

Bridge discovery approach

censys

Shodan

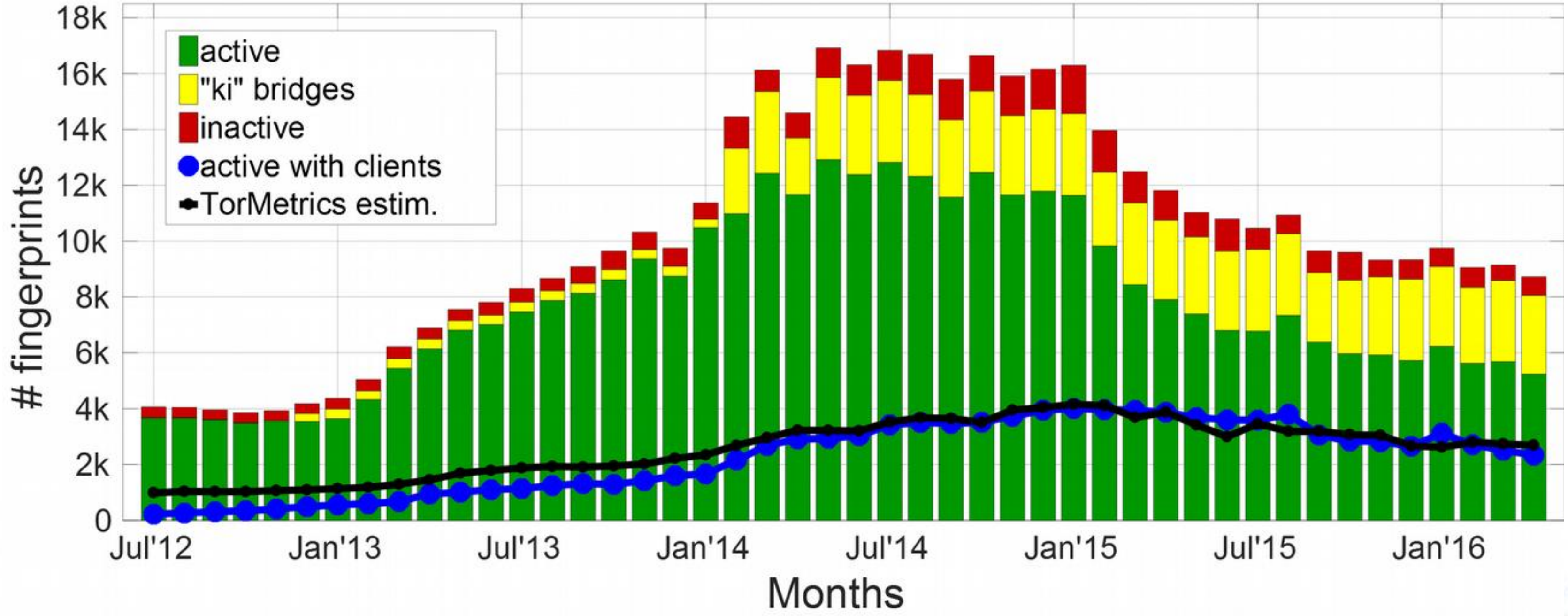
1. Finding candidate IP addresses
2. Filtering relays COLLECTor
3. Verifying IP addresses
4. Identifying private proxies

   (check descriptor)

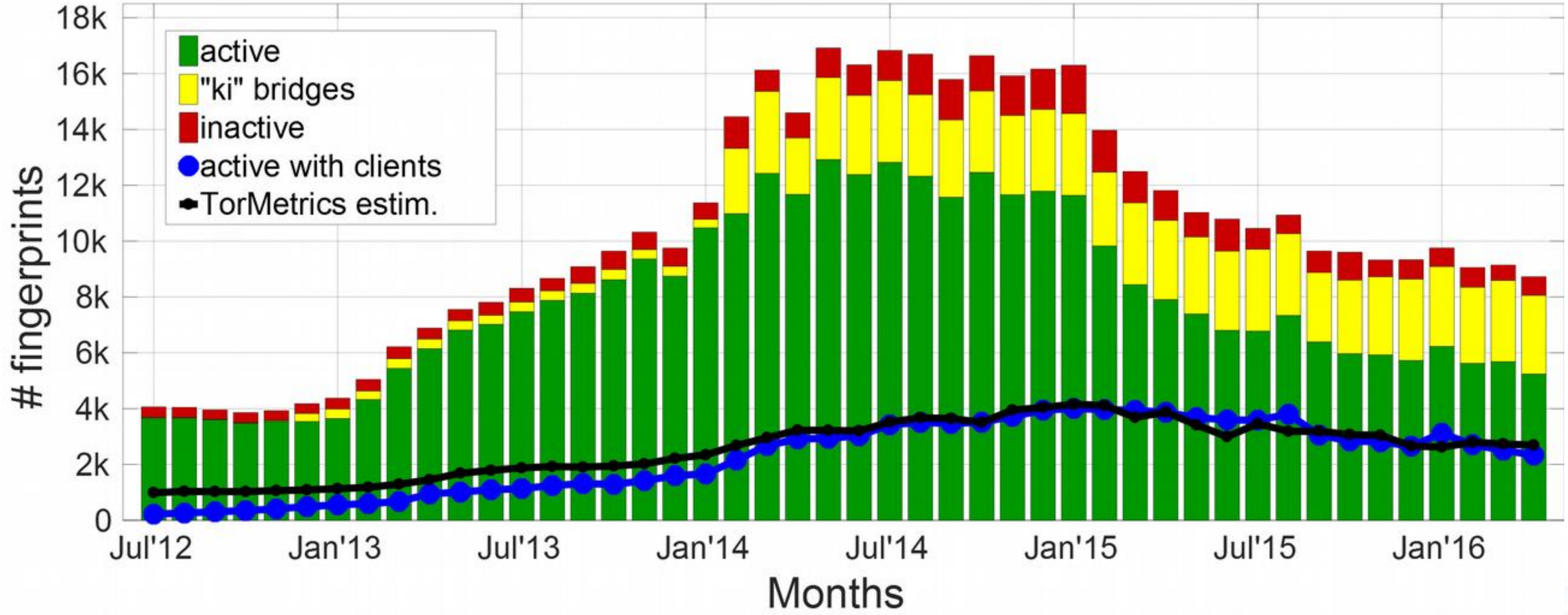
5. Classifying as public or private bridge COLLECTor

   (find sanitized fingerprint)

Public bridges – population



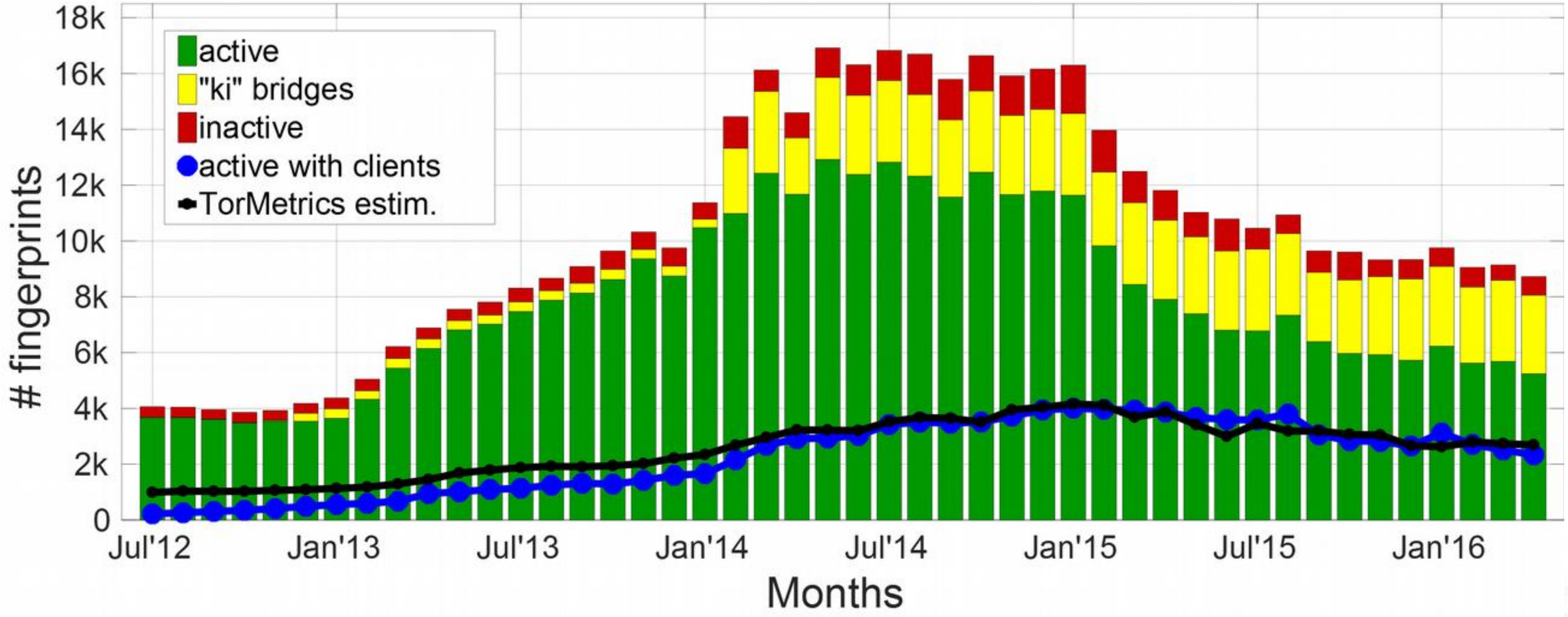
Public bridges – population



April 2016:

- 5.3K active public bridges
- 2.3K bridges with clients

Public bridges – population

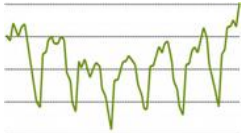


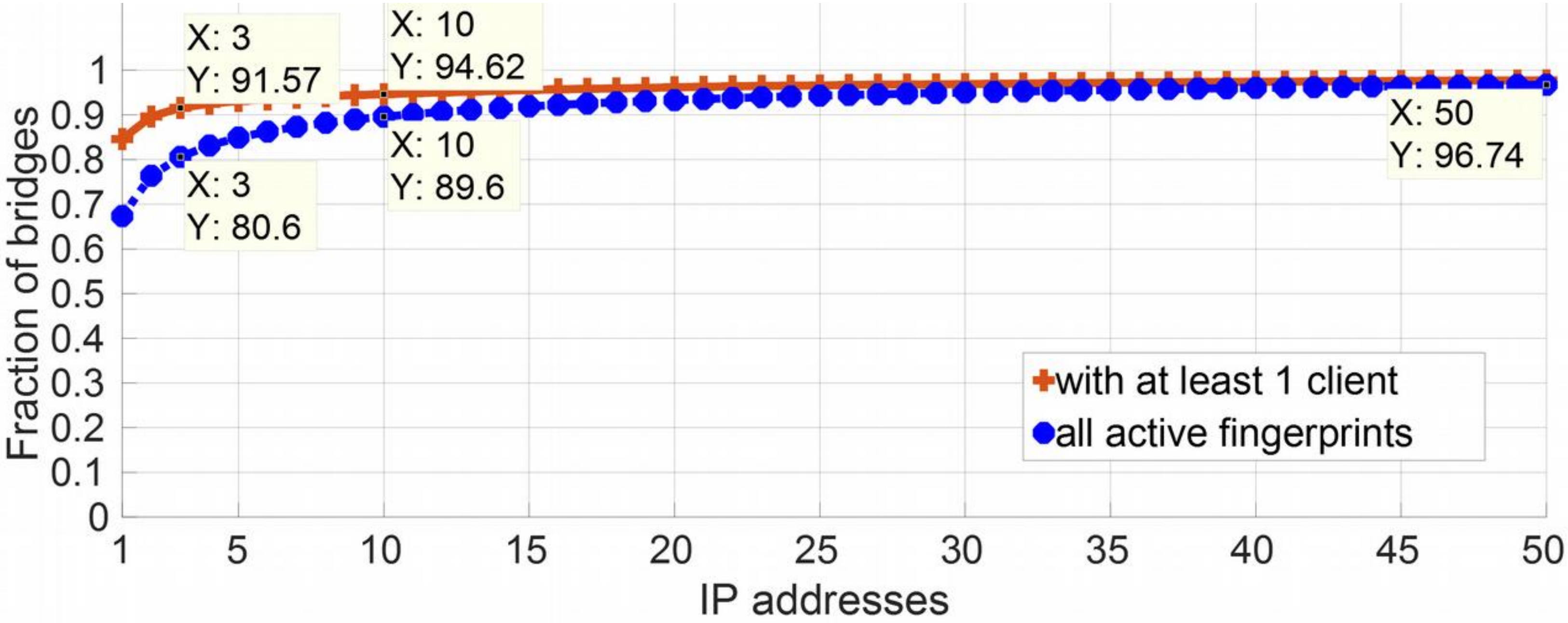
April 2016:

- 5.3K active public bridges
- 2.3K bridges with clients

Different population metrics!

Public bridges – stability



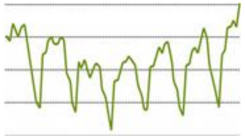


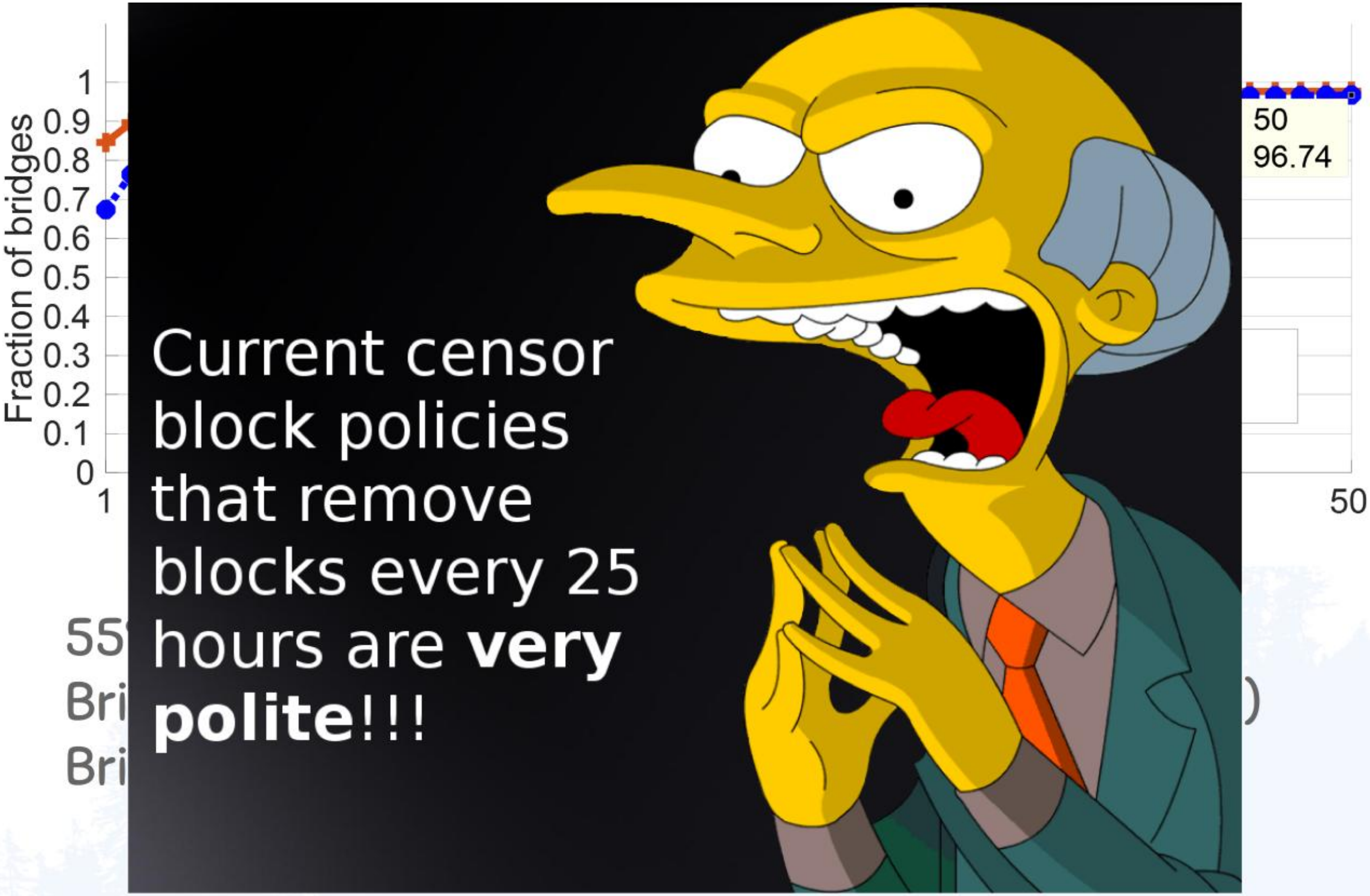
55% of the bridges live < 1 day → No clients

Bridges with clients long lived → 4 months (median)

Bridges with clients rarely change IP address

Public bridges – stability





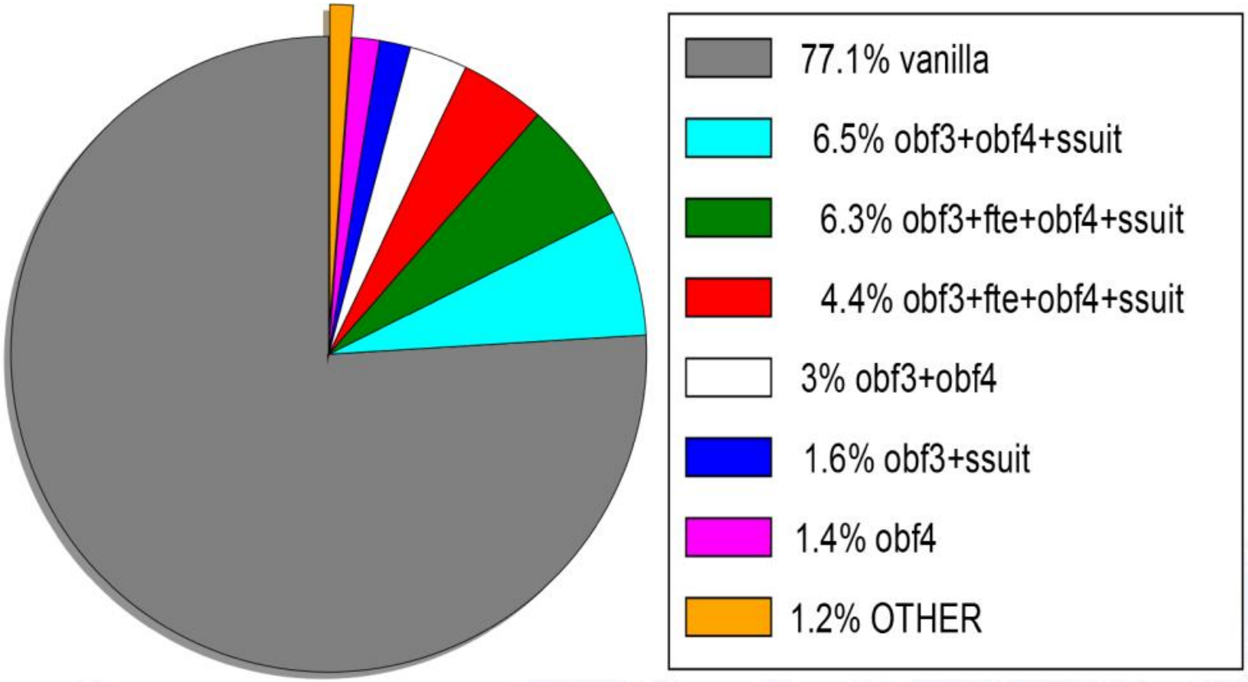
Current censor block policies that remove blocks every 25 hours are **very polite**!!!

55

Bri)

Bri

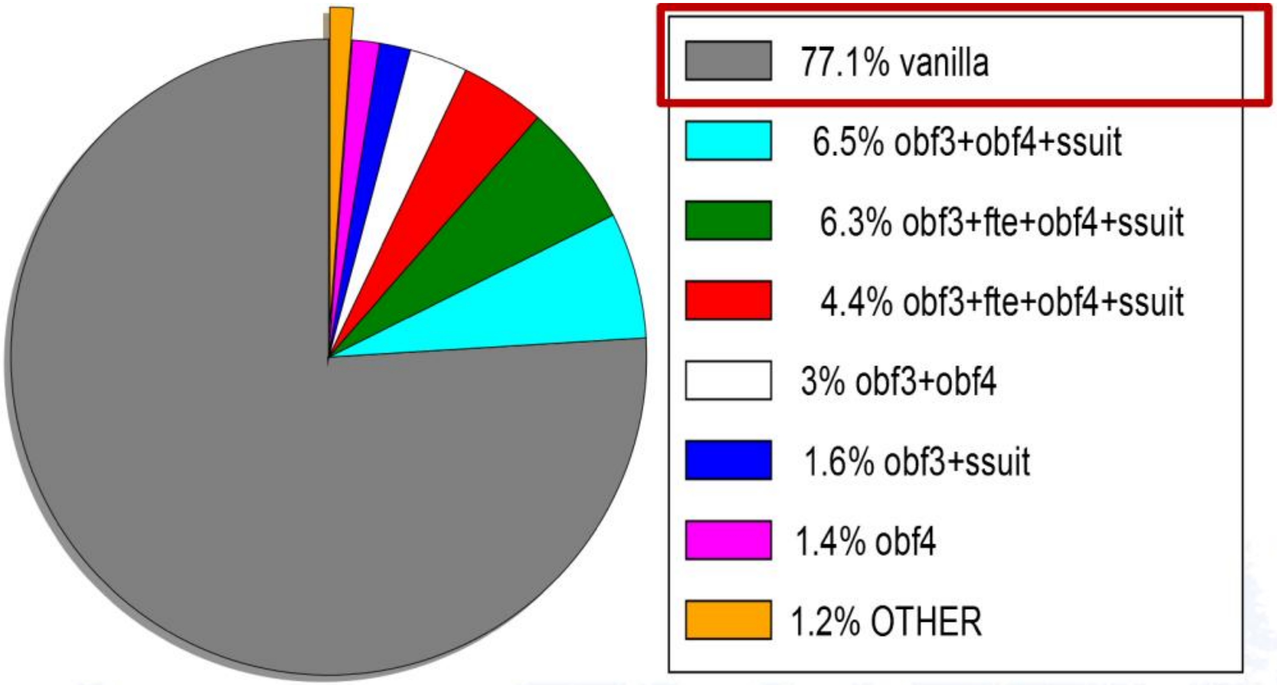
Public bridges – PT deployment



April 2016

Public bridges – PT deployment

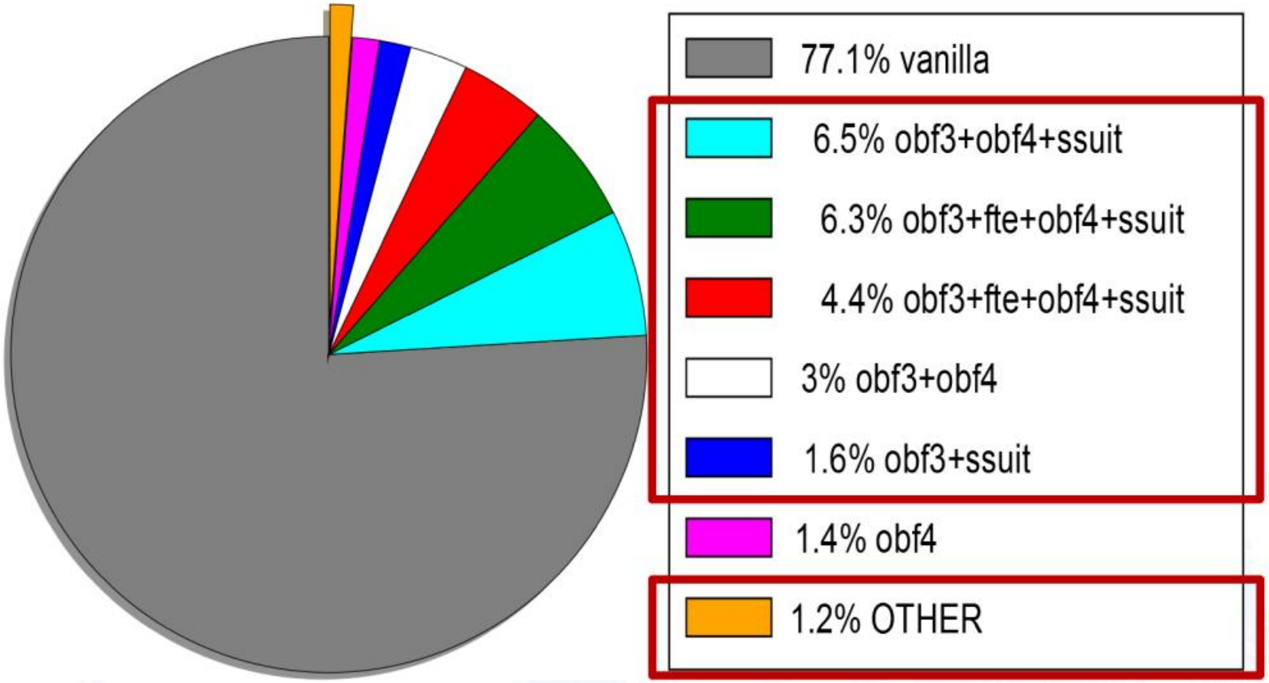
April 2016



Blockable!

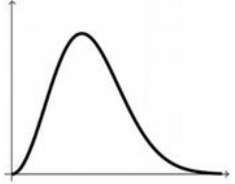
Public bridges – PT deployment

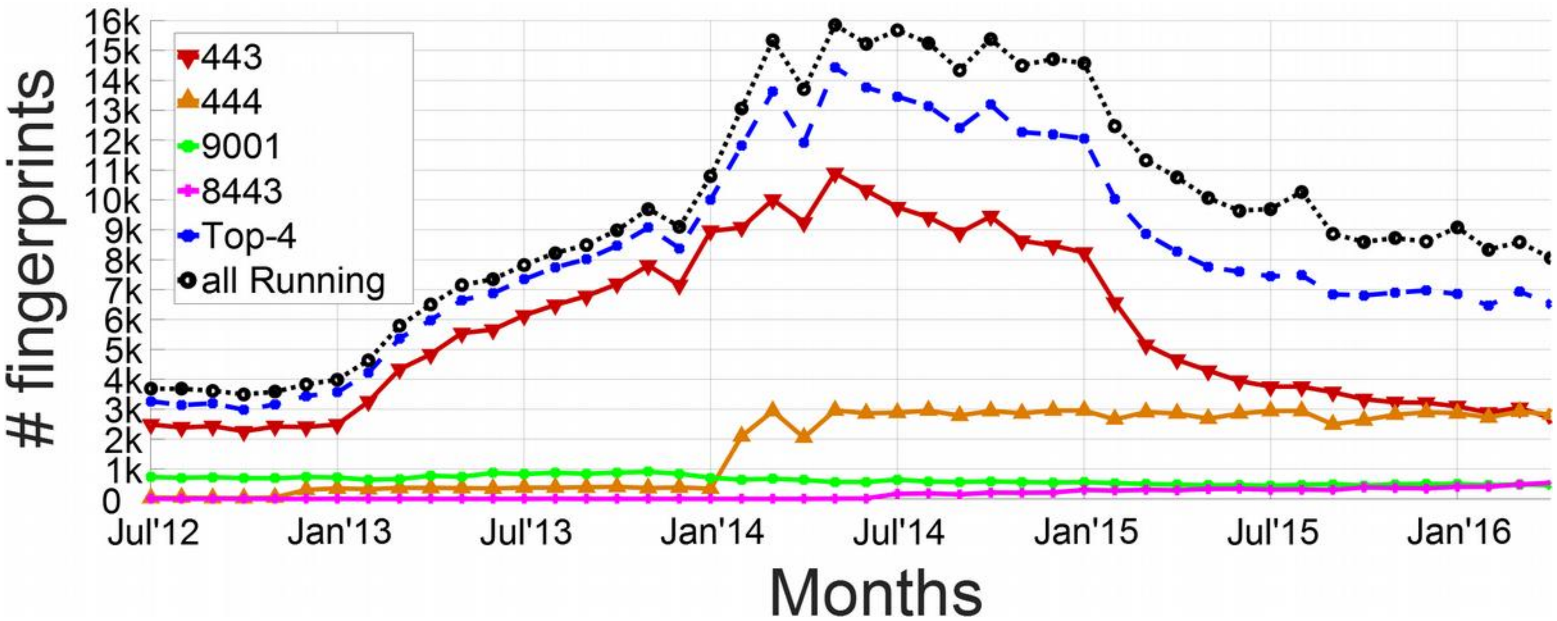
April 2016



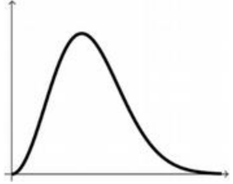
Conflicting security properties!

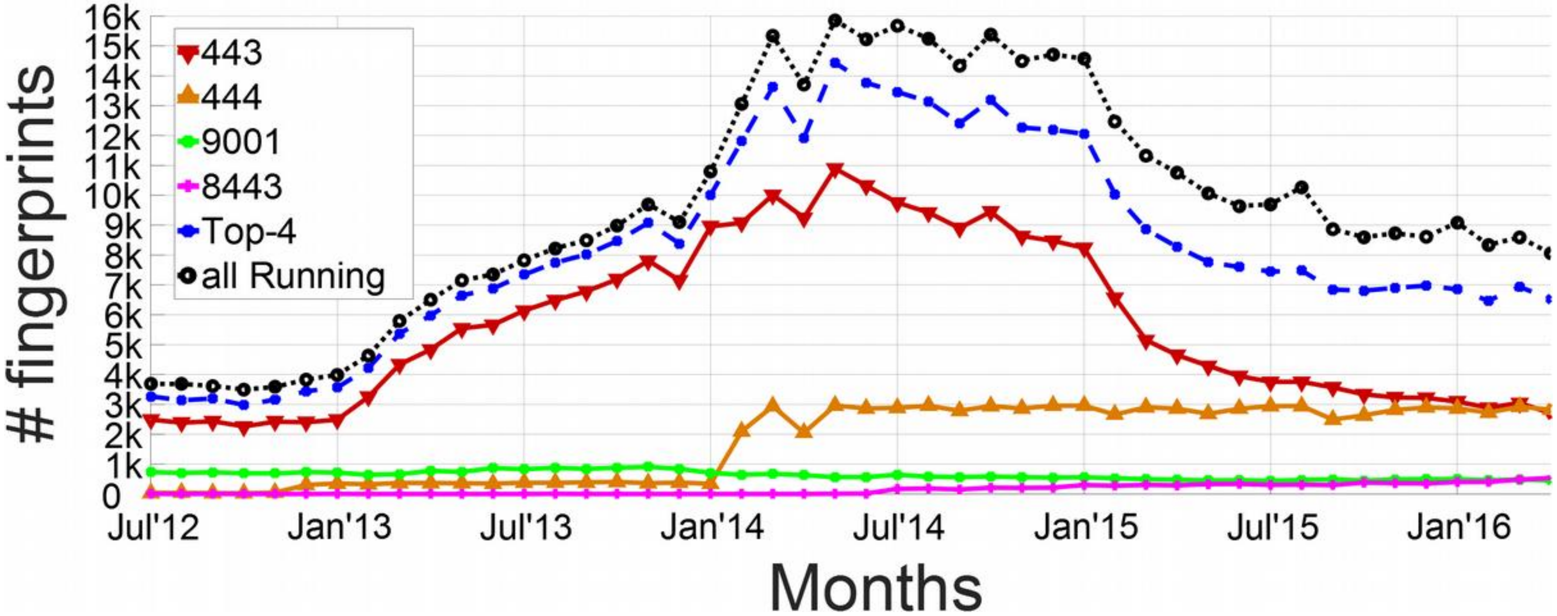
Public bridges – OR port distribution





Public bridges – OR port distribution

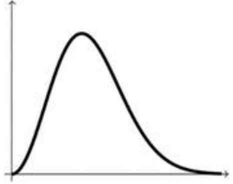


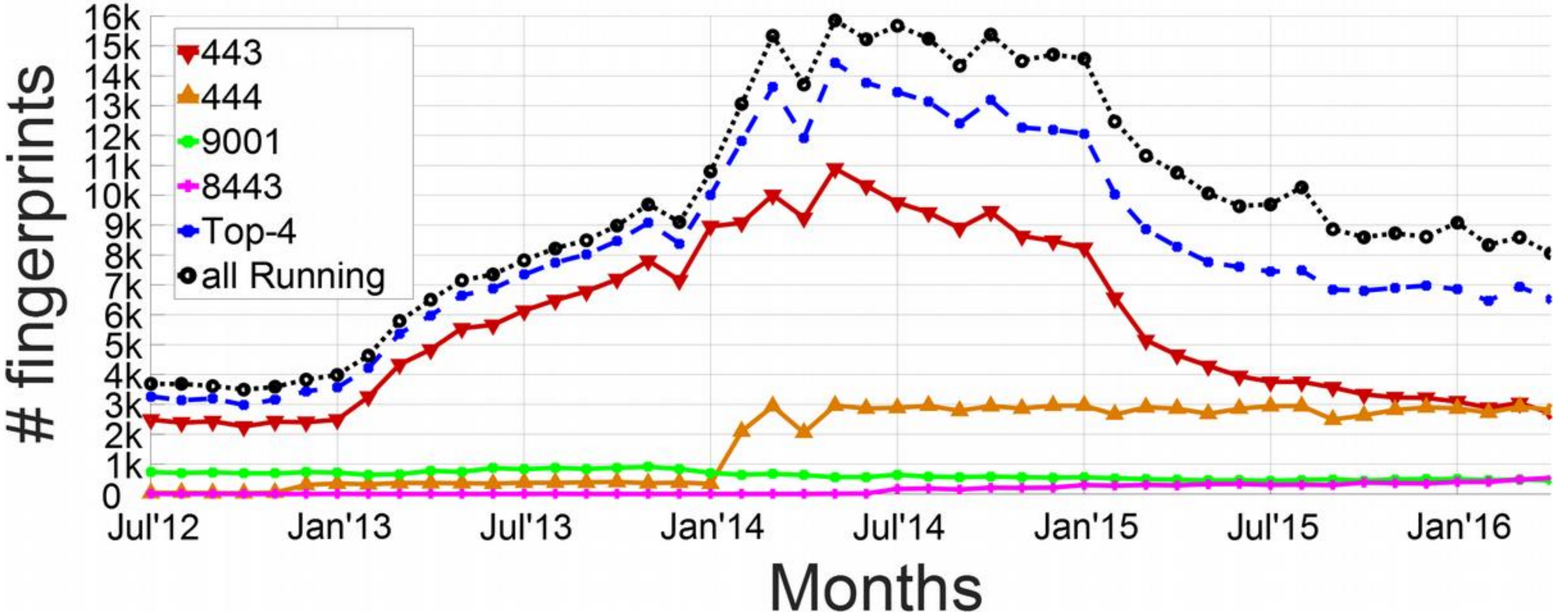


Top-3 OR ports (¬444) are used by 71% of public bridges

(99% of active fingerprints never change their OR port)

Public bridges – OR port distribution



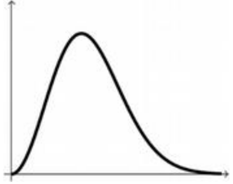


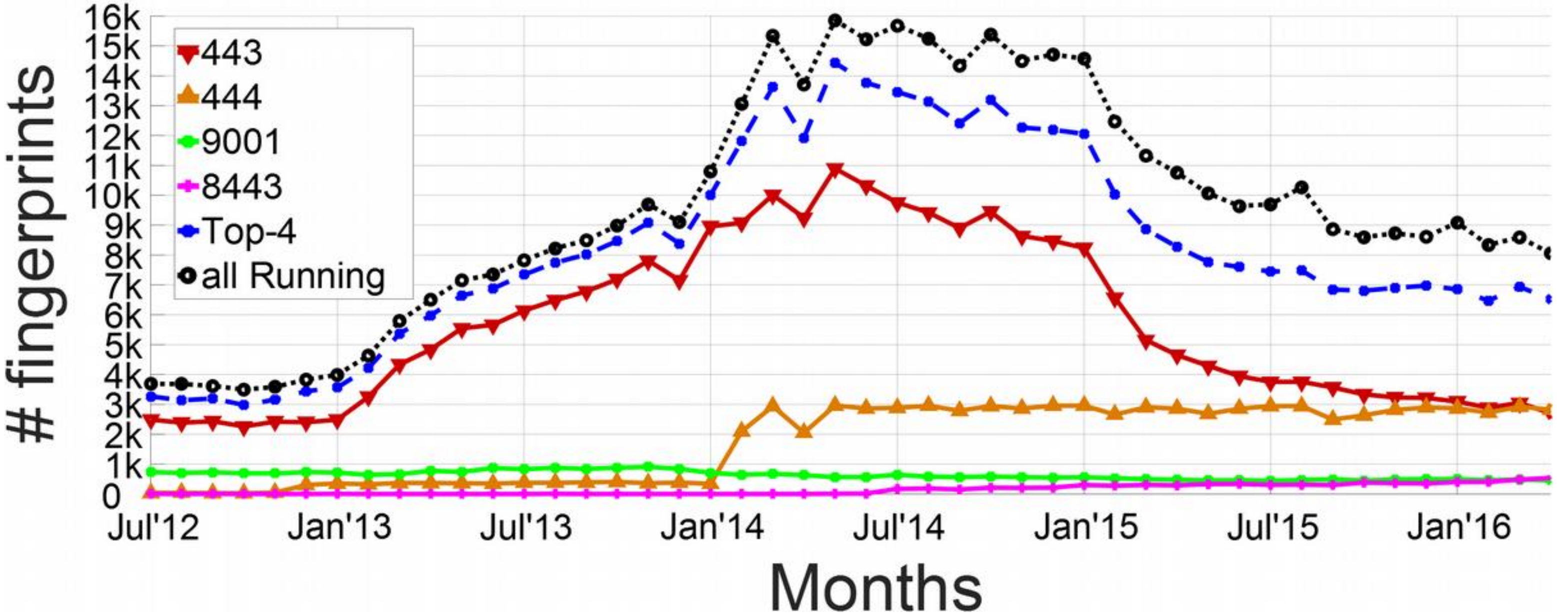
Top-3 OR ports (¬444) are used by 71% of public bridges

(99% of active fingerprints never change their OR port)

Scanning on those ports reveals majority of bridges!

Public bridges – OR port distribution





Top-3 OR ports (¬444) are used by 71% of public bridges

(99% of active fingerprints never change their OR port)

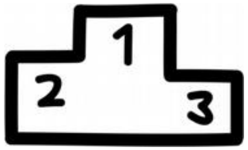
Scanning on those ports reveals majority of bridges!

COLLECTor

Public bridges – Ranking

Not all bridges are equally important!!

Public bridges – Ranking

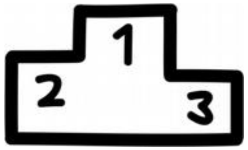


Not all bridges are equally important!!

How well is country-level blocking working?
Which bridges should censor target next?

CC	Used Brid.	Top 20 (Default)
cn	712	45.6% (44.0%)
ir	941	86.6% (86.1%)
sy	74	76.9% (68.0%)
uk	943	84.1% (84.0%)
us	1,496	58.7% (56.7%)
All	2,213	91.71% (91.4%)

Public bridges – Ranking



Not all bridges are equally important!!

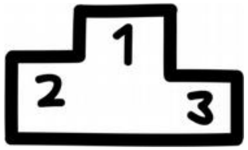
How well is country-level blocking working?
Which bridges should censor target next?

CC	Used Brid.	Top 20 (Default)
cn	712	45.6% (44.0%)
ir	941	86.6% (86.1%)
sy	74	76.9% (68.0%)
uk	943	84.1% (84.0%)
us	1,496	58.7% (56.7%)
All	2,213	91.71% (91.4%)

91% traffic used default bridges!

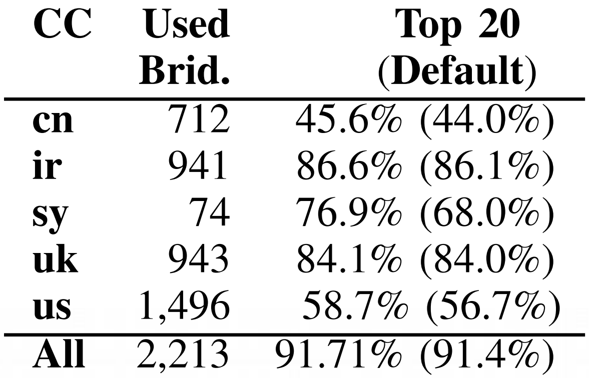
A censor can disconnect users in reaction to an event

Public bridges – Ranking



Not all bridges are equally important!!

How well is country-level blocking working?
Which bridges should censor target next?

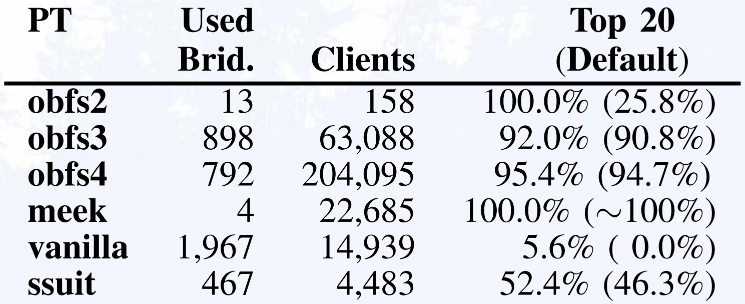


CC	Used Brid.	Top 20 (Default)
cn	712	45.6% (44.0%)
ir	941	86.6% (86.1%)
sy	74	76.9% (68.0%)
uk	943	84.1% (84.0%)
us	1,496	58.7% (56.7%)
All	2,213	91.71% (91.4%)

91% traffic used default bridges!

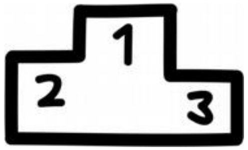
A censor can disconnect users in reaction to an event

How well is blocking of specific PT working?



PT	Used Brid.	Clients	Top 20 (Default)
obfs2	13	158	100.0% (25.8%)
obfs3	898	63,088	92.0% (90.8%)
obfs4	792	204,095	95.4% (94.7%)
meek	4	22,685	100.0% (∼100%)
vanilla	1,967	14,939	5.6% (0.0%)
ssuit	467	4,483	52.4% (46.3%)

Public bridges – Ranking



Not all bridges are equally important!!

How well is country-level blocking working?
Which bridges should censor target next?

CC	Used Brid.	Top 20 (Default)
cn	712	45.6% (44.0%)
ir	941	86.6% (86.1%)
sy	74	76.9% (68.0%)
uk	943	84.1% (84.0%)
us	1,496	58.7% (56.7%)
All	2,213	91.71% (91.4%)

91% traffic used default bridges!

A censor can disconnect users in reaction to an event

How well is blocking of specific PT working?

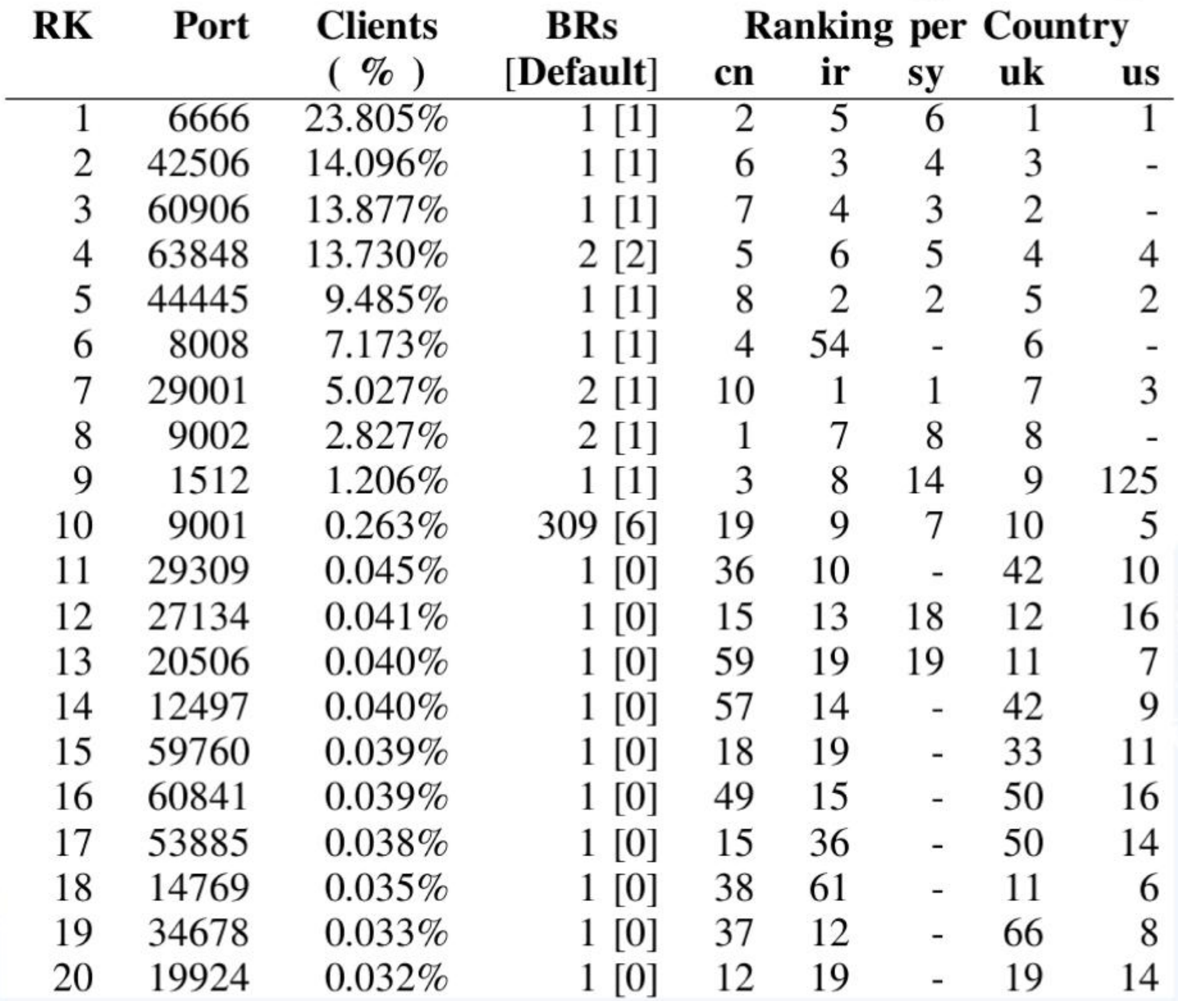
PT	Used Brid.	Clients	Top 20 (Default)
obfs2	13	158	100.0% (25.8%)
obfs3	898	63,088	92.0% (90.8%)
obfs4	792	204,095	95.4% (94.7%)
meek	4	22,685	100.0% (∼100%)
vanilla	1,967	14,939	5.6% (0.0%)
ssuit	467	4,483	52.4% (46.3%)

94% obs4 in default!

Useless reply protection...

Public bridges – Ranking

Not all OR ports are equally important!!



RK	Port	Clients (%)	BRs [Default]	Ranking per Country cn	 ir	 sy	 uk	 us
1	6666	23.805%	1 [1]	2	5	6	1	1
2	42506	14.096%	1 [1]	6	3	4	3	-
3	60906	13.877%	1 [1]	7	4	3	2	-
4	63848	13.730%	2 [2]	5	6	5	4	4
5	44445	9.485%	1 [1]	8	2	2	5	2
6	8008	7.173%	1 [1]	4	54	-	6	-
7	29001	5.027%	2 [1]	10	1	1	7	3
8	9002	2.827%	2 [1]	1	7	8	8	-
9	1512	1.206%	1 [1]	3	8	14	9	125
10	9001	0.263%	309 [6]	19	9	7	10	5
11	29309	0.045%	1 [0]	36	10	-	42	10
12	27134	0.041%	1 [0]	15	13	18	12	16
13	20506	0.040%	1 [0]	59	19	19	11	7
14	12497	0.040%	1 [0]	57	14	-	42	9
15	59760	0.039%	1 [0]	18	19	-	33	11
16	60841	0.039%	1 [0]	49	15	-	50	16
17	53885	0.038%	1 [0]	15	36	-	50	14
18	14769	0.035%	1 [0]	38	61	-	11	6
19	34678	0.033%	1 [0]	37	12	-	66	8
20	19924	0.032%	1 [0]	12	19	-	19	14

Private bridges – Population (Apr 2016)

Port	SC	Source	Disc.	Verified	Public	Private	Proxy
443	9	Censys	2,448	1,315 (1,122)	897 (860)	263 (262)	164
993	2	Censys	19	16 (13)	11 (11)	3 (2)	2
995	3	Censys	14	14 (13)	10 (10)	3 (3)	1
444	1	Shodan	14	12 (101)	8 (97)	1 (4)	4
8443	1	Shodan	191	156 (149)	148 (148)	1 (1)	7
9001	1	Shodan	2,001	1047 (587)	165 (166)	415 (421)	468
9002	1	Shodan	23	19 (5)	1 (1)	4 (4)	14
All	17	All	4,684	2,554 (1,986)	1,239 (1,292)	684 (694)	645

Private bridges – Population (Apr 2016)

Port	SC	Source	Disc.	Verified	Public	Private	Proxy
443	9	Censys	2,448	1,315 (1,122)	897 (860)	263 (262)	164
993	2	Censys	19	16 (13)	11 (11)	3 (2)	2
995	3	Censys	14	14 (13)	10 (10)	3 (3)	1
444	1	Shodan	14	12 (101)	8 (97)	1 (4)	4
8443	1	Shodan	191	156 (149)	148 (148)	1 (1)	7
9001	1	Shodan	2,001	1047 (587)	165 (166)	415 (421)	468
9002	1	Shodan	23	19 (5)	1 (1)	4 (4)	14
All	17	All	4,684	2,554 (1,986)	1,239 (1,292)	684 (694)	645

Deanonymized 35% public bridges with clients

Private bridges – Population (Apr 2016)

Port	SC	Source	Disc.	Verified	Public	Private	Proxy
443	9	Censys	2,448	1,315 (1,122)	897 (860)	263 (262)	164
993	2	Censys	19	16 (13)	11 (11)	3 (2)	2
995	3	Censys	14	14 (13)	10 (10)	3 (3)	1
444	1	Shodan	14	12 (101)	8 (97)	1 (4)	4
8443	1	Shodan	191	156 (149)	148 (148)	1 (1)	7
9001	1	Shodan	2,001	1047 (587)	165 (166)	415 (421)	468
9002	1	Shodan	23	19 (5)	1 (1)	4 (4)	14
All	17	All	4,684	2,554 (1,986)	1,239 (1,292)	684 (694)	645

Deanonymized 35% public bridges with clients

Found 684 private bridges + 645 private proxies

Private bridges - Population (Apr 2016)

Port	SC	Source	Disc.	Verified	Public	Private	Proxy
443	9	Censys	2,448	1,315 (1,122)	897 (860)	263 (262)	164
993	2	Censys	19	16 (13)	11 (11)	3 (2)	2
995	3	Censys	14	14 (13)	10 (10)	3 (3)	1
444	1	Shodan	14	12 (101)	8 (97)	1 (4)	4
8443	1	Shodan	191	156 (149)	148 (148)	1 (1)	7
9001	1	Shodan	2,001	1047 (587)	165 (166)	415 (421)	468
9002	1	Shodan	23	19 (5)	1 (1)	4 (4)	14
All	17	All	4,684	2,554 (1,986)	1,239 (1,292)	684 (694)	645

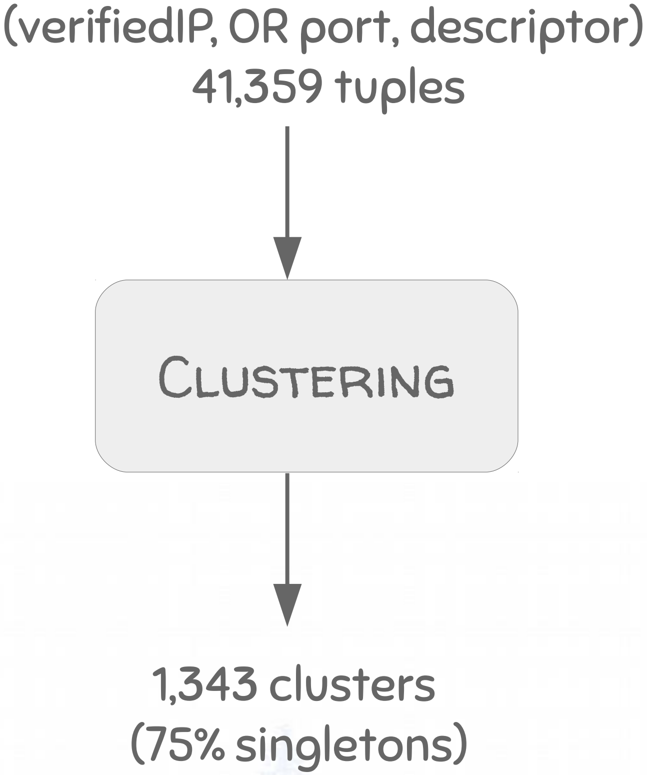
Deanonymized 35% public bridges with clients

Found 684 private bridges + 645 private proxies

175 non-public domains in contact info

(307 bridges - 187 public /180 private)

Private bridges – clustering



(verifiedIP, OR port, descriptor)
41,359 tuples

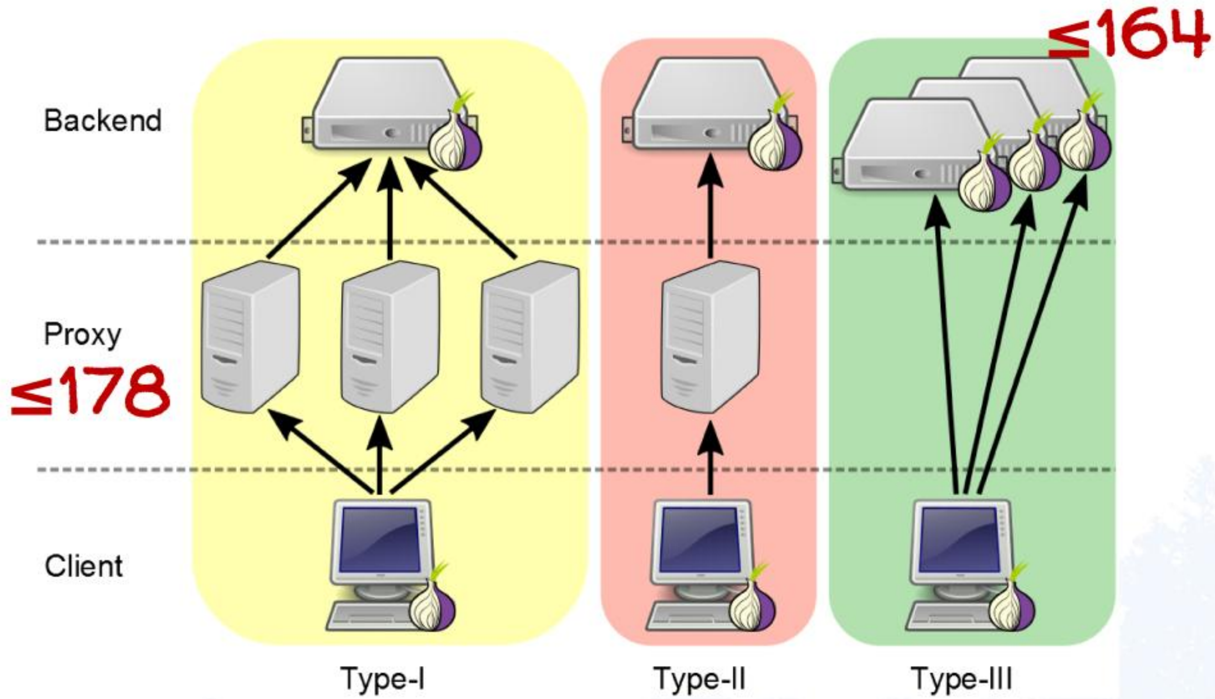
Clustering

1,343 clusters
(75% singletons)

Features:

- Same fingerprint
- Similar nicknames
- Same contact information
- Similar verified IP address (+ identical config)
- Simlar IP address in descriptor (+ identical config)

Private bridges – clustering

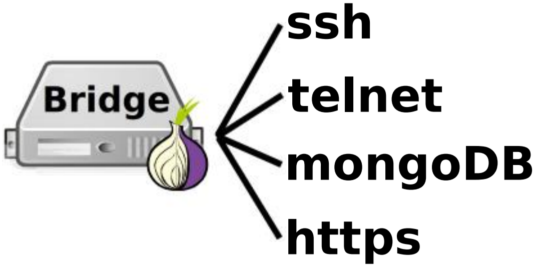


Type-I	: 47
Type-II	: 138
Type-III	: 88
Type-IV	: 43
Type-V	: 10
Mixed	: 16

77% Proxies and Backend in same AS

Proxies do not provide IP diversity

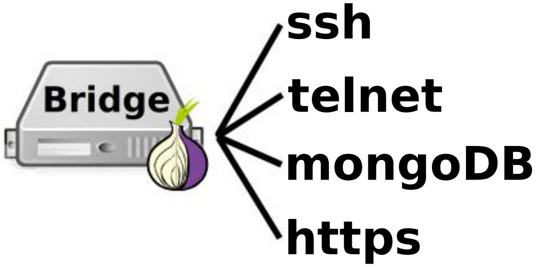
Bonus track – tracking bridges



Shodan

621 / 2,554 verified IPs (24%) offer at least one additional service and 10% more than one.

Bonus track – tracking bridges



ssh

telnet

mongoDB

https

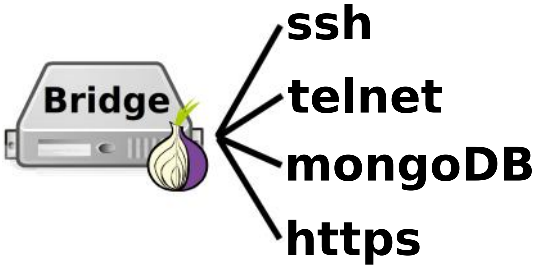
Shodan

621 / 2,554 verified IPs (24%) offer at least one additional service and 10% more than one.

Most common additional services:

- SSH – ports 22 and 2222,
- Web services – ports 80 and 443
- RPC port mapper – port 111

Bonus track – tracking bridges



SHODAN

621 / 2,554 verified IPs (24%) offer at least one additional service and 10% more than one.

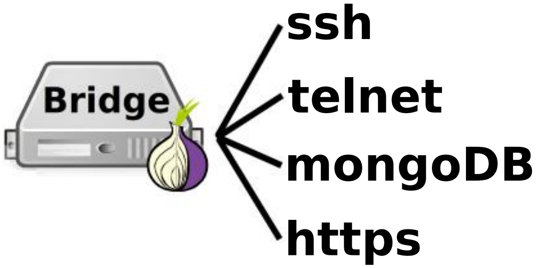
Most common additional services:

- SSH – ports 22 and 2222,
- Web services – ports 80 and 443
- RPC port mapper – port 111

} Unique identifiers

- SSH keys
- Certificate serial numbers

Bonus track – tracking bridges



Bridge

ssh

telnet

mongoDB

https

SHODAN

621 / 2,554 verified IPs (24%) offer at least one additional service and 10% more than one.

Most common additional services:

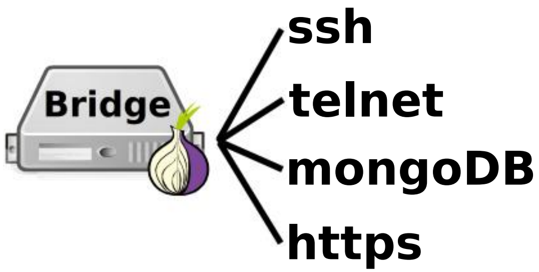
- SSH – ports 22 and 2222,
- Web services – ports 80 and 443
- RPC port mapper – port 111

Unique identifiers

- SSH keys
- Certificate serial numbers

SHODAN

Bonus track – tracking bridges



Bridge

ssh

telnet

mongoDB

https

SHODAN

621 / 2,554 verified IPs (24%) offer at least one additional service and 10% more than one.

Most common additional services:

- SSH – ports 22 and 2222,
- Web services – ports 80 and 443
- RPC port mapper – port 111

Unique identifiers

- SSH keys
- Certificate serial numbers

SHODAN

2248 candidate IPs

- 248 bridges
- 9 **new** bridges!
- (e.g., change IP within Amazon EC2)

Conclusion – Security Implications

Public Bridges

- Bridges with clients live 4 months, no IP changes → Blocking
- PTs with conflicting security properties
- Top-3 OR ports 71% public bridges → Patch CollecTor
- 91% bridge traffic uses default bridges → Defeats purpose
- Bridge Ranking enables targeted attacks

Conclusion – Security Implications

Public Bridges

- Bridges with clients live 4 months, no IP changes → Blocking
- PTs with conflicting security properties
- Top-3 OR ports 71% public bridges → Patch CollecTor
- 91% bridge traffic uses default bridges → Defeats purpose
- Bridge Ranking enables targeted attacks

Bridge discovery

- Deanonymized 35% of public bridges
- Found 684 private bridges + 645 private proxies
- 35% bridges are private
- Clusters of bridges+proxies deployed → Little IP diversity

Conclusion – Security Implications

Public Bridges

- Bridges with clients live 4 months, no IP changes → Blocking
- PTs with conflicting security properties
- Top-3 OR ports 71% public bridges → Patch CollecTor
- 91% bridge traffic uses default bridges → Defeats purpose
- Bridge Ranking enables targeted attacks

Bridge discovery

- Deanonymized 35% of public bridges
- Found 684 private bridges + 645 private proxies
- 35% bridges are private
- Clusters of bridges+proxies deployed → Little IP diversity

Open OR Port needs fixing!!!!