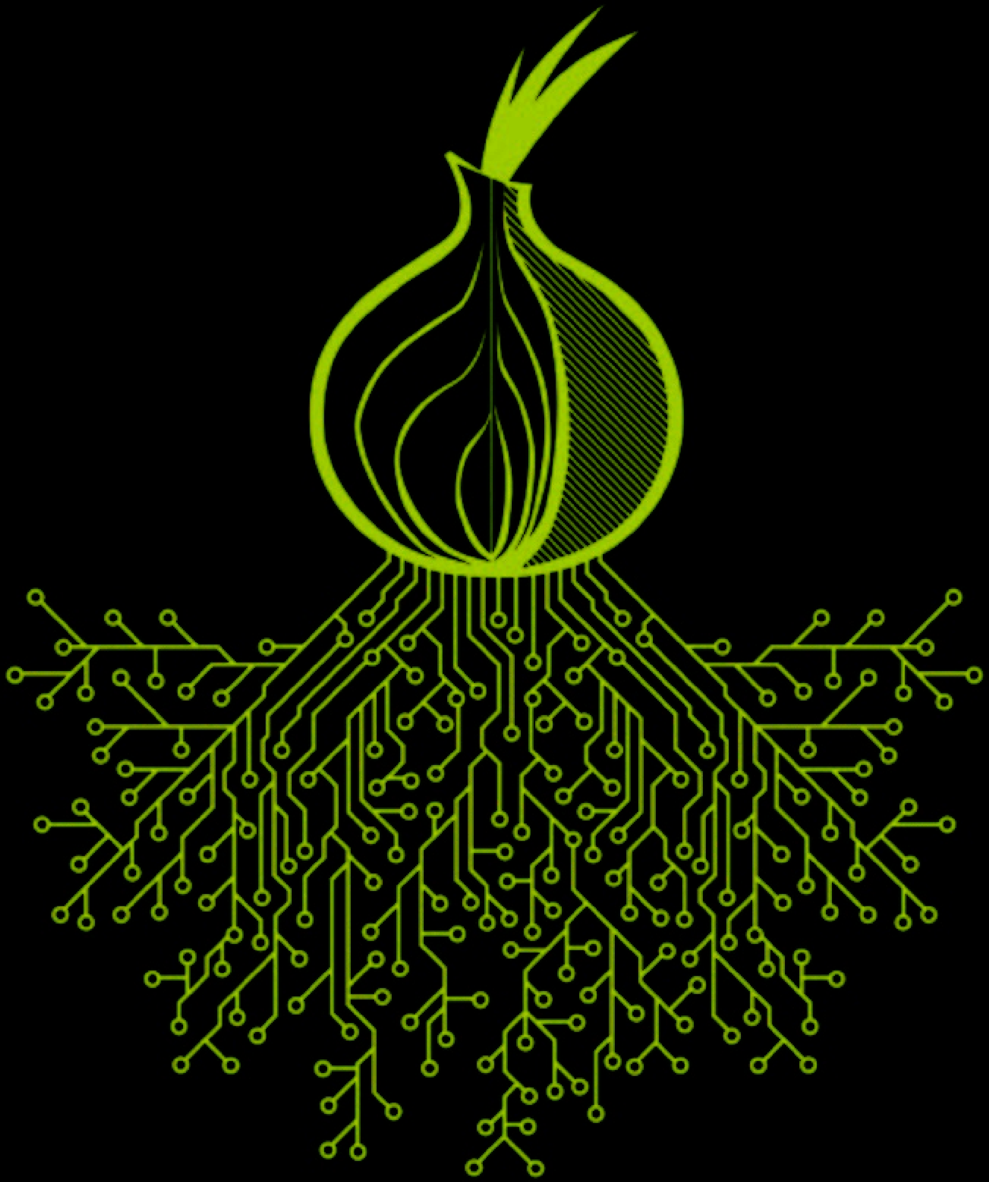
The Tor Project



Our mission is to advance human rights and freedoms by creating and deploying free and open privacy and anonymity technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding.

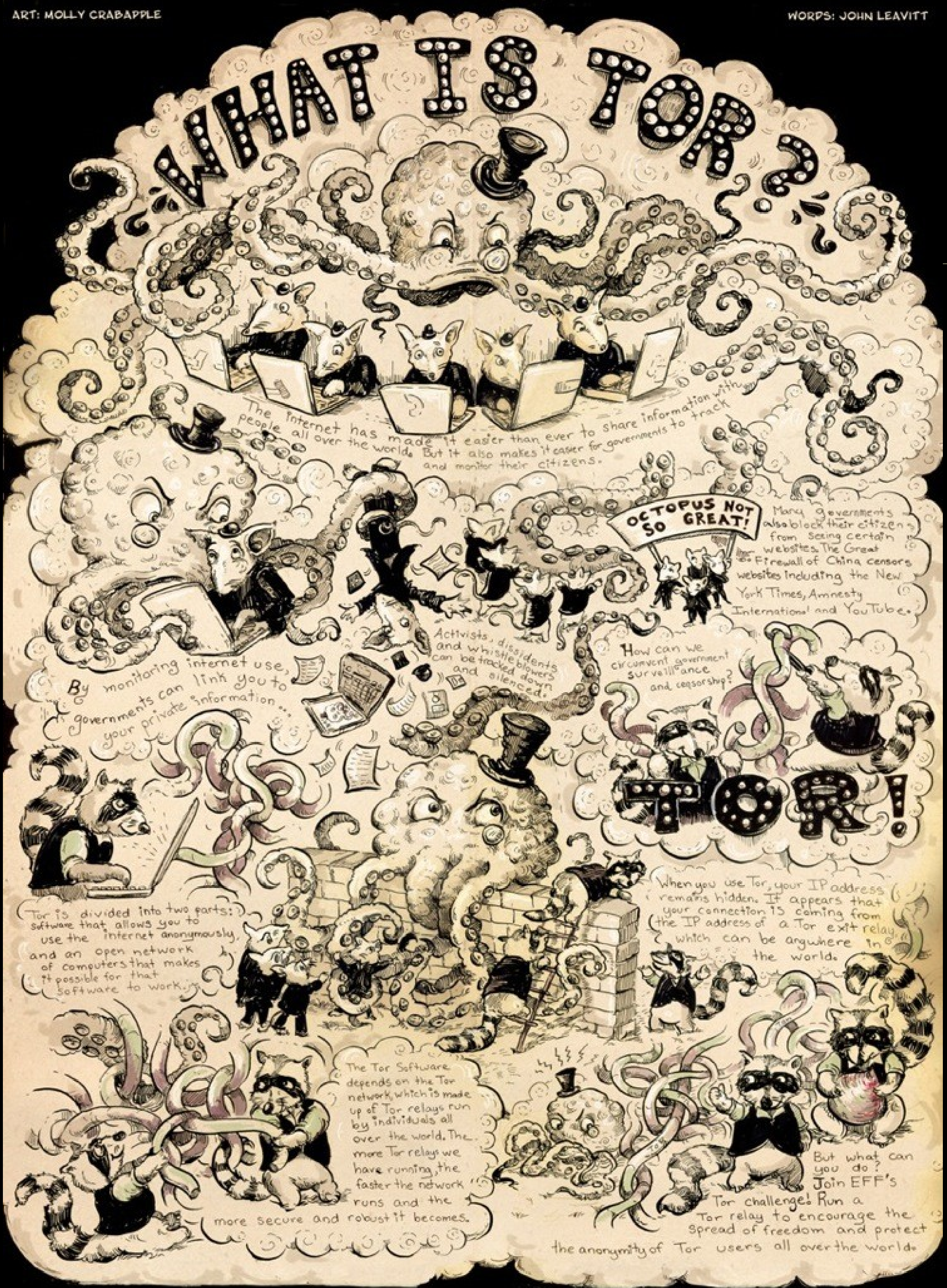
Metadata

Data about data

"Metadata was traditionally in the card catalogs of libraries"

-- Wikipedia

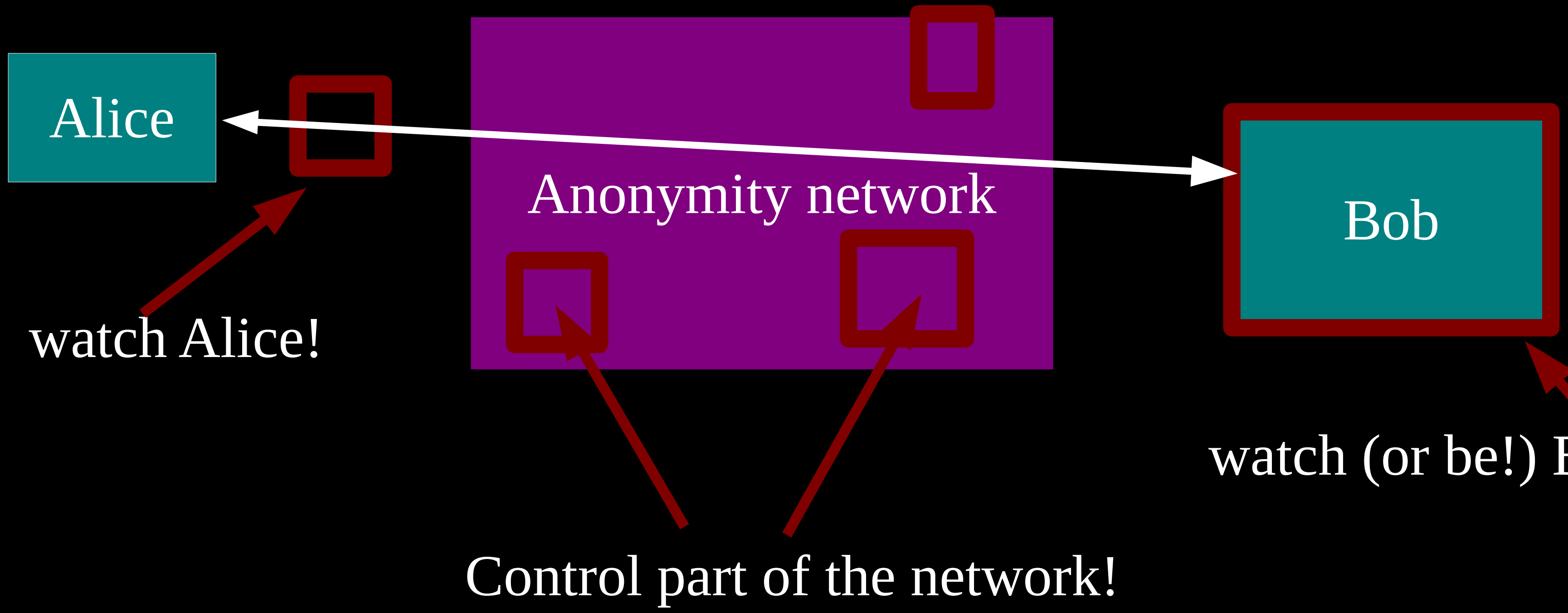
"We kill people based on metadata"


ART: MOLLY CRABAPPLE
WORDS: JOHN LEAVITT
WHAT IS TOR?
The Internet has made it easier than ever to share information with people all over the world. But it also makes it easier for governments to track and monitor their citizens.
OCTOPUS NOT SO GREAT!
Many governments also block their citizens from seeing certain websites. The Great Firewall of China censors websites including the New York Times, Amnesty International and YouTube.
By monitoring internet use, governments can link you to your private information...
Activists, dissidents and whistle blowers can be tracked down and silenced.
How can we circumvent government surveillance and censorship?
TOR!
When you use Tor, your IP address remains hidden. It appears that your connection is coming from the IP address of a Tor exit relay which can be anywhere in the world.
Tor is divided into two parts: software that allows you to use the internet anonymously, and an open network of computers that makes it possible for that software to work.
The Tor Software depends on the Tor network, which is made up of Tor relays run by individuals all over the world. The more Tor relays we have running, the faster the network runs and the more secure and robust it becomes.
But what can you do? Join EFF's Tor challenge! Run a Tor relay to encourage the spread of freedom and protect the anonymity of Tor users all over the world.

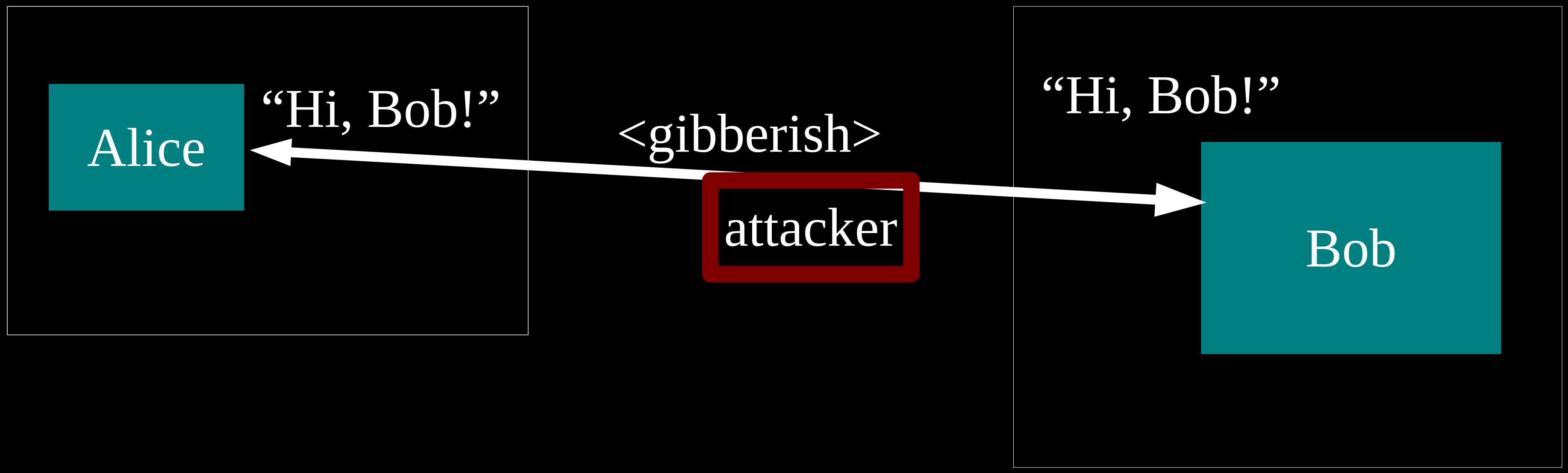
- Online Anonymity
  - Open Source
  - Open Network
- Community of researchers, developers, users and relay operators.
- U.S. 501(c)(3) non-profit organization

Estimated 2,000,000+
daily Tor users

Threat model: what can the attacker do?



Anonymity isn't encryption: Encryption just protects contents.



Privacy by promise, privacy by design

“You can't prove it was me!”

“Promise you won't look!”

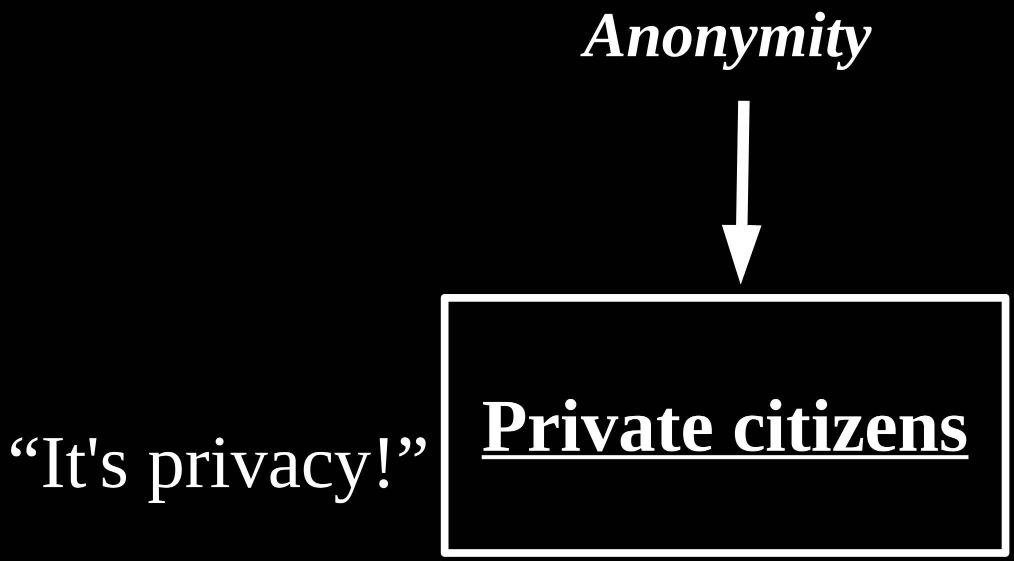
“Promise you won't remember!”

“Promise you won't tell!”

“I didn't write my name on it!”

“Isn't the Internet already anonymous?”

Anonymity serves different interests for different user groups.

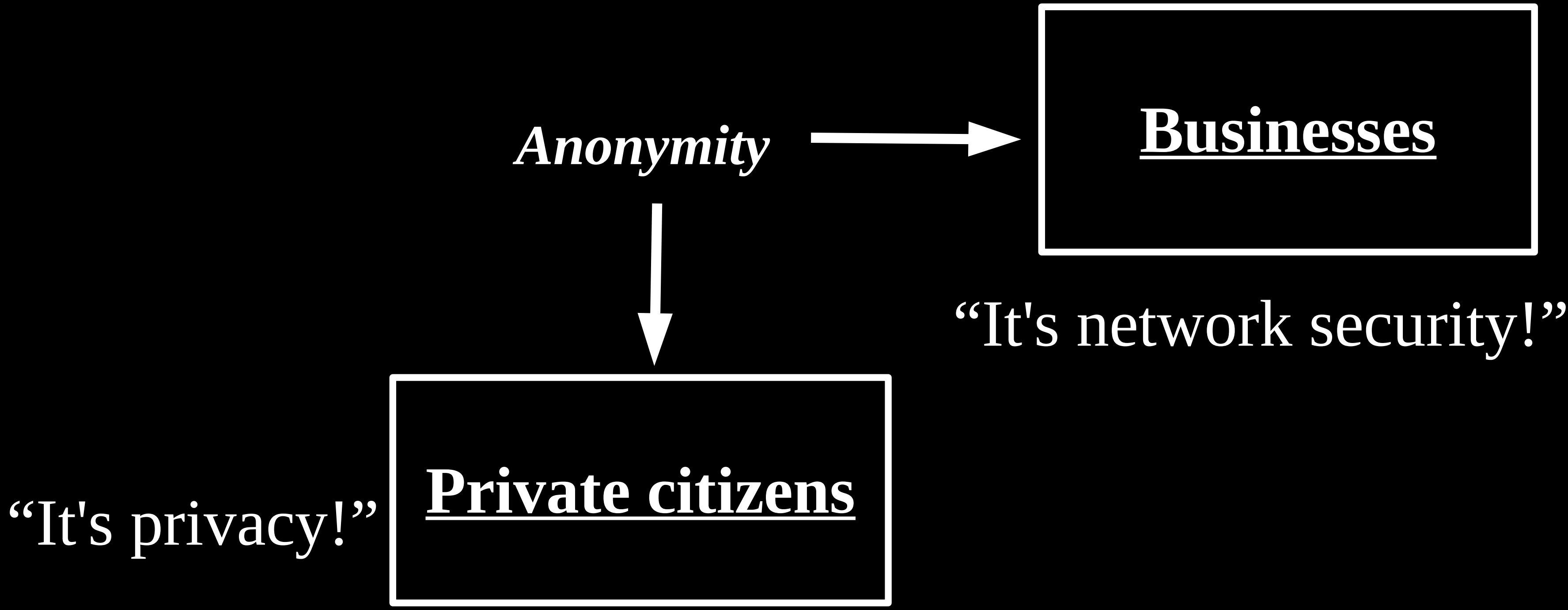


Anonymity

“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Anonymity

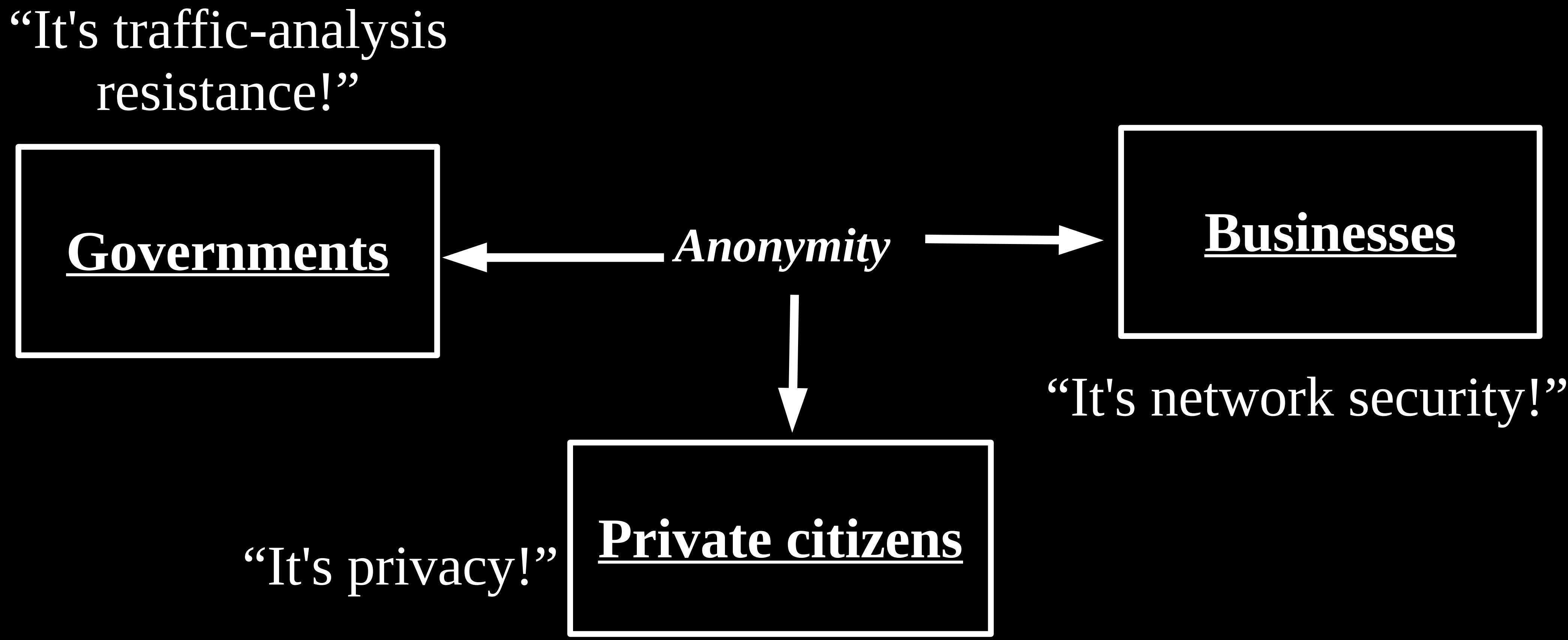
Businesses

"It's network security!"

Private citizens

"It's privacy!"

Anonymity serves different interests for different user groups.



“It's traffic-analysis resistance!”

Governments

Anonymity

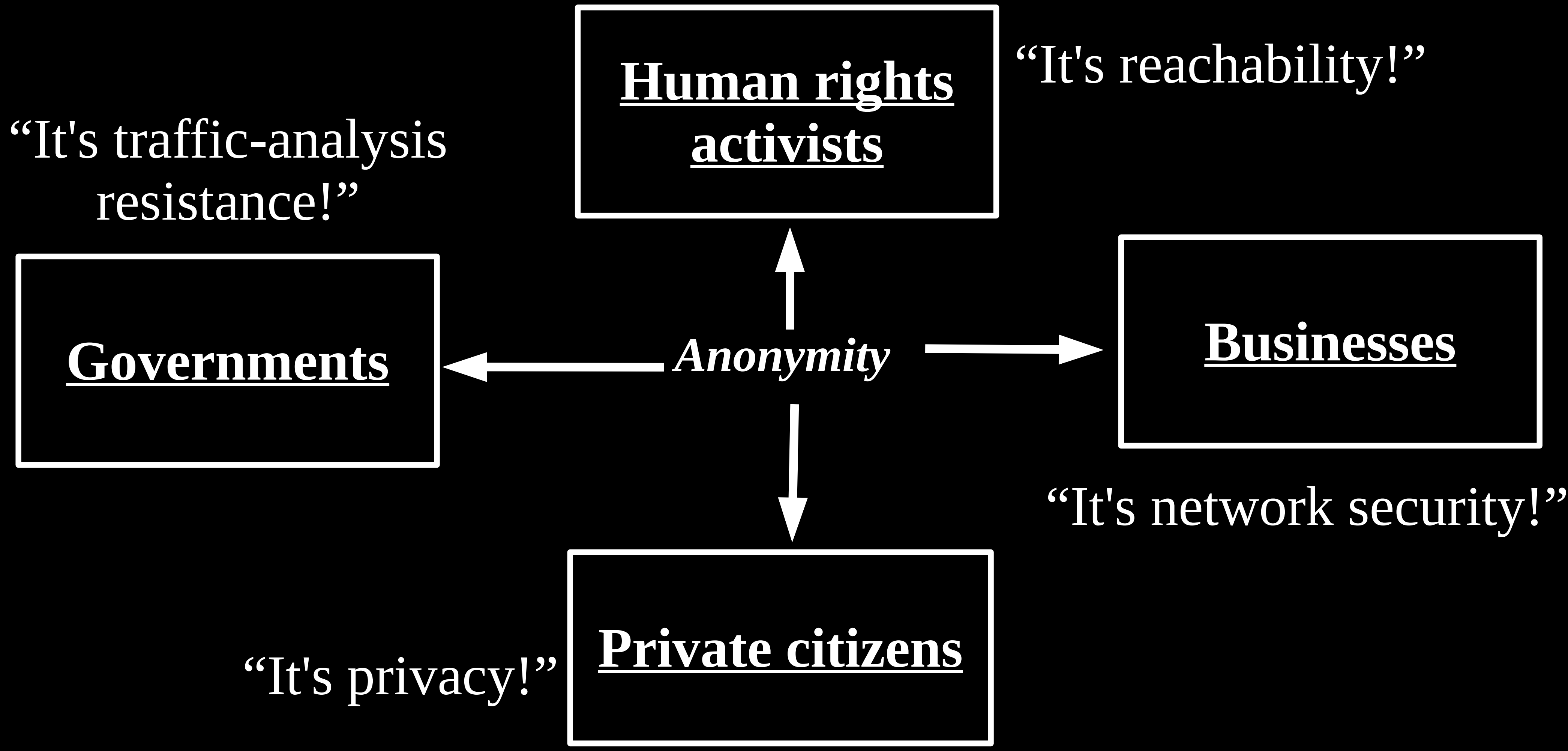
Businesses

“It's network security!”

“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Human rights activists

"It's reachability!"

"It's traffic-analysis resistance!"

Governments

Anonymity

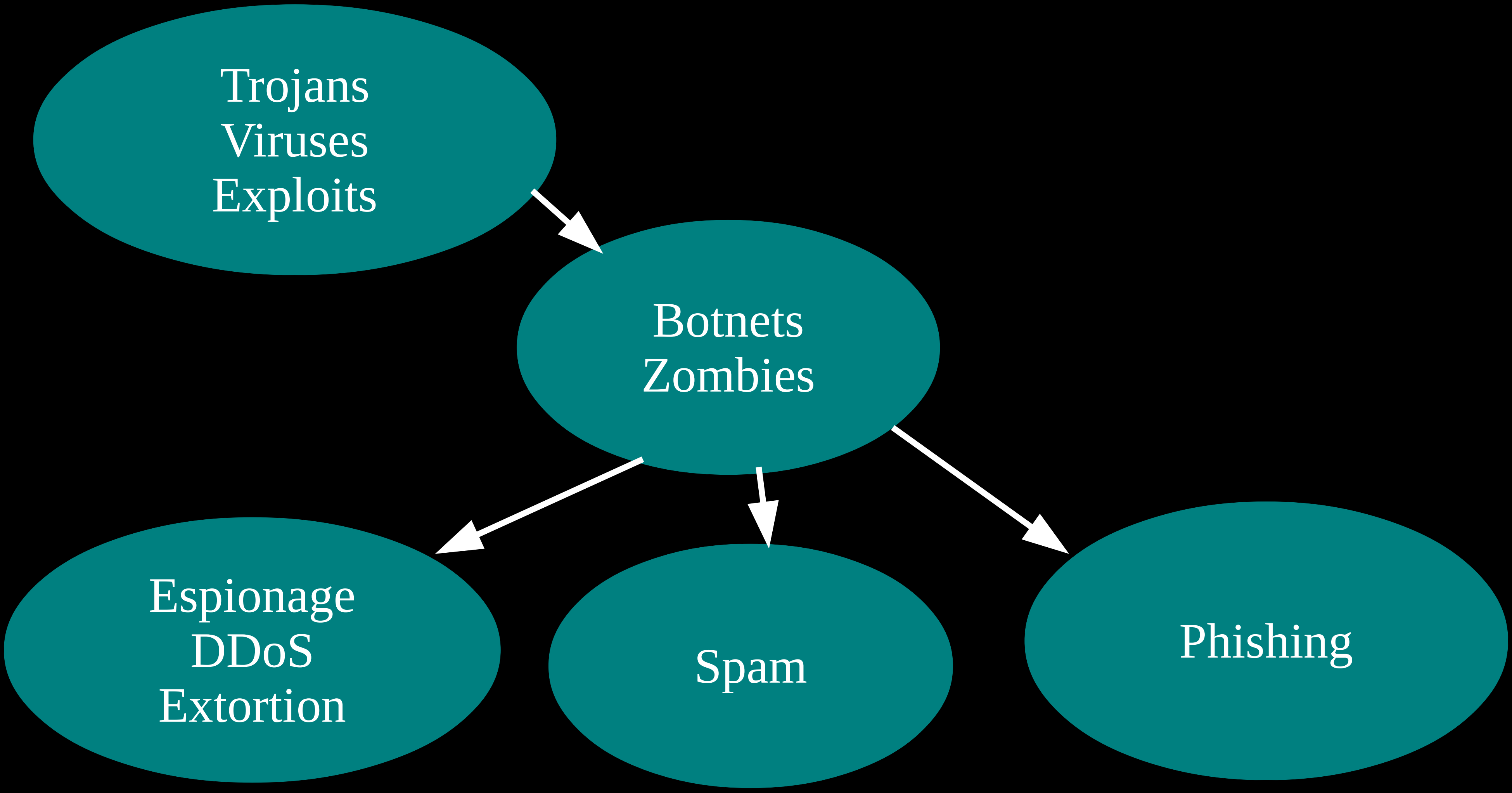
Businesses

"It's network security!"

"It's privacy!"

Private citizens

Current situation: Bad people on the Internet are doing fine



Trojans
Viruses
Exploits

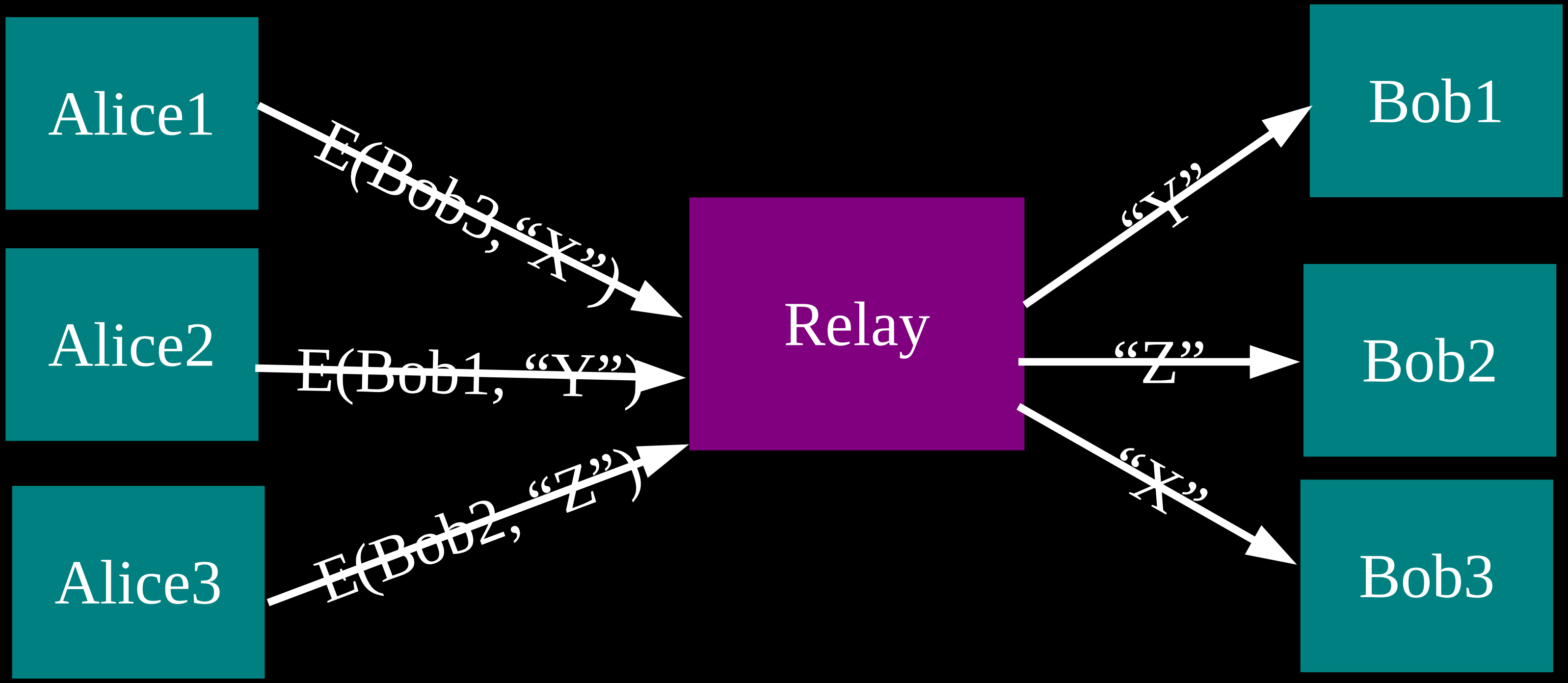
Botnets
Zombies

Espionage
DDoS
Extortion

Spam

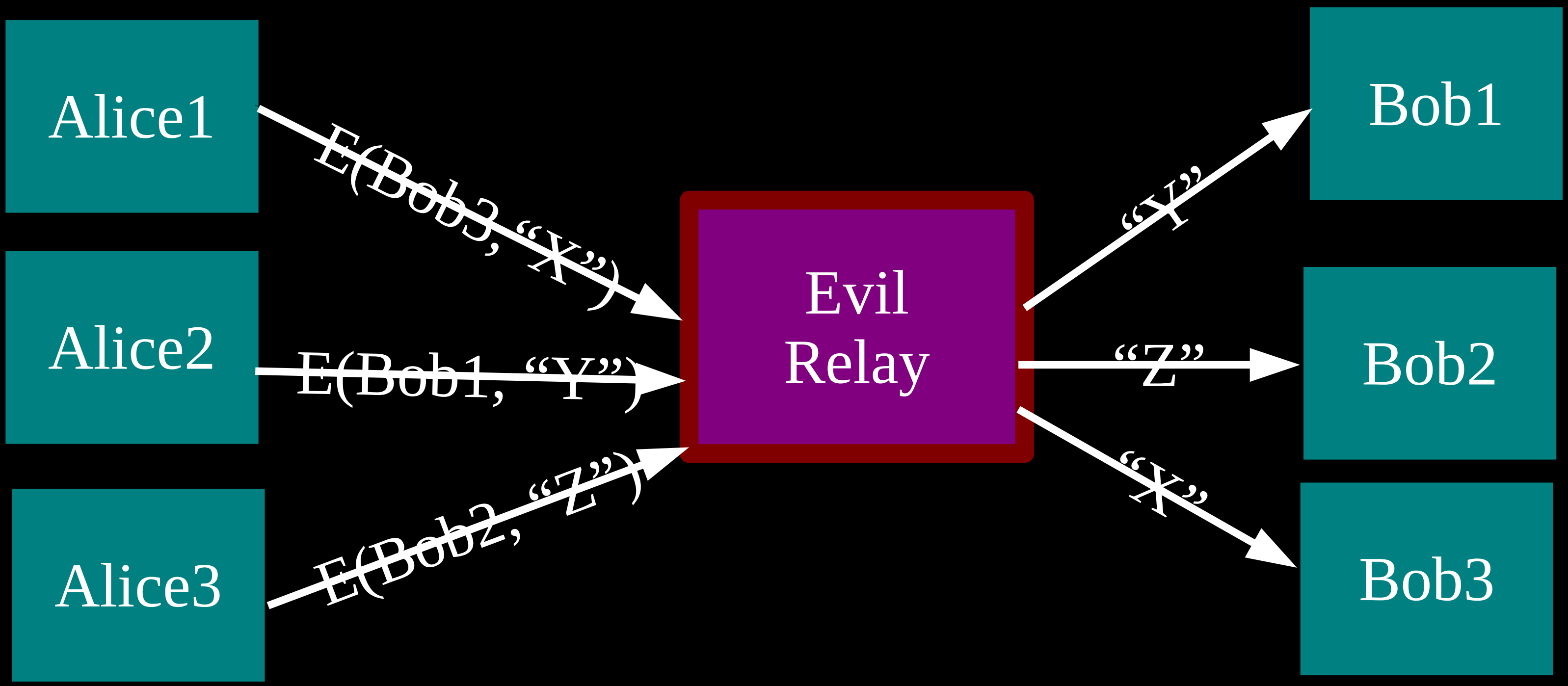
Phishing

The simplest designs use a single relay to hide connections.

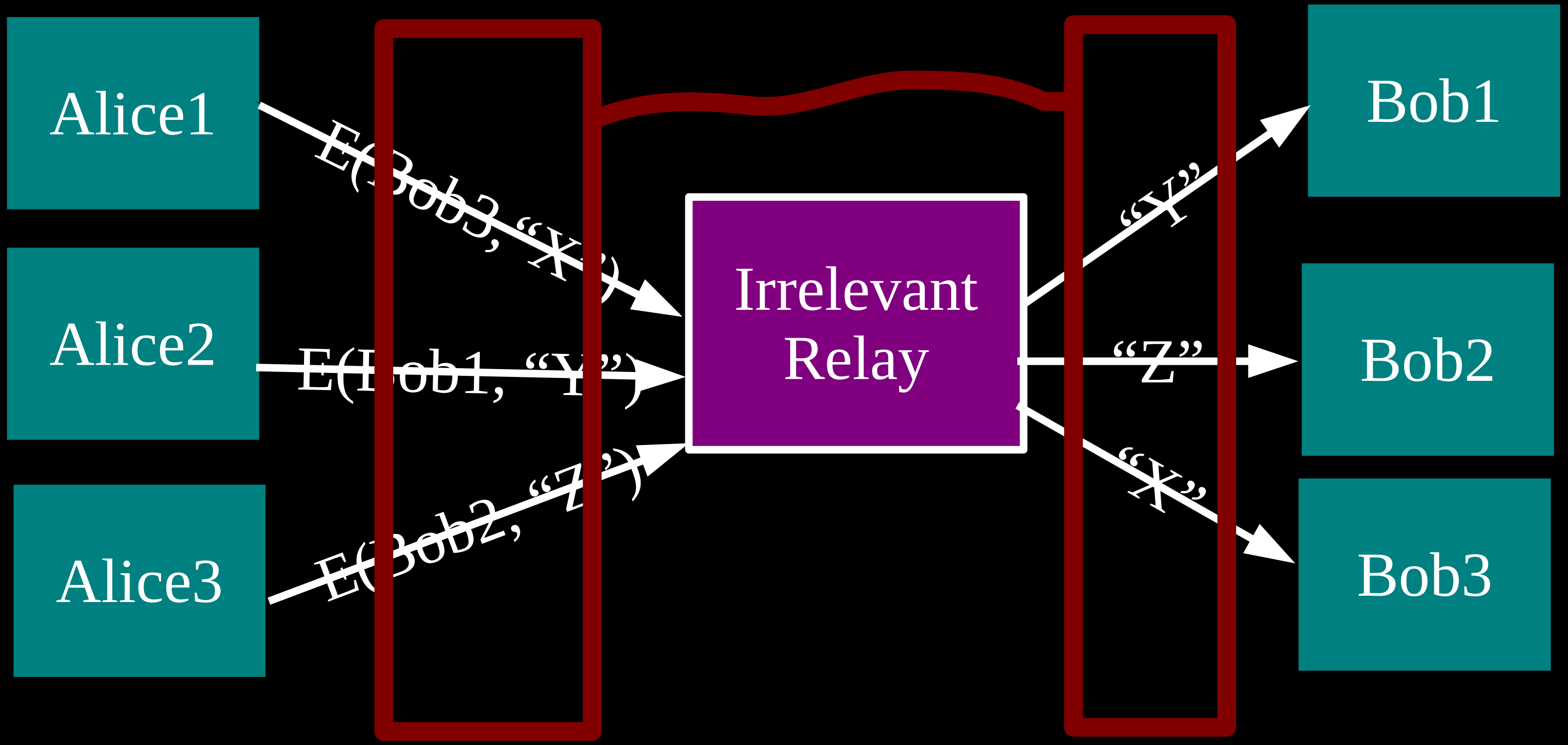


(example: some commercial proxy providers)

But a single relay (or eavesdropper!) is a single point of failure.

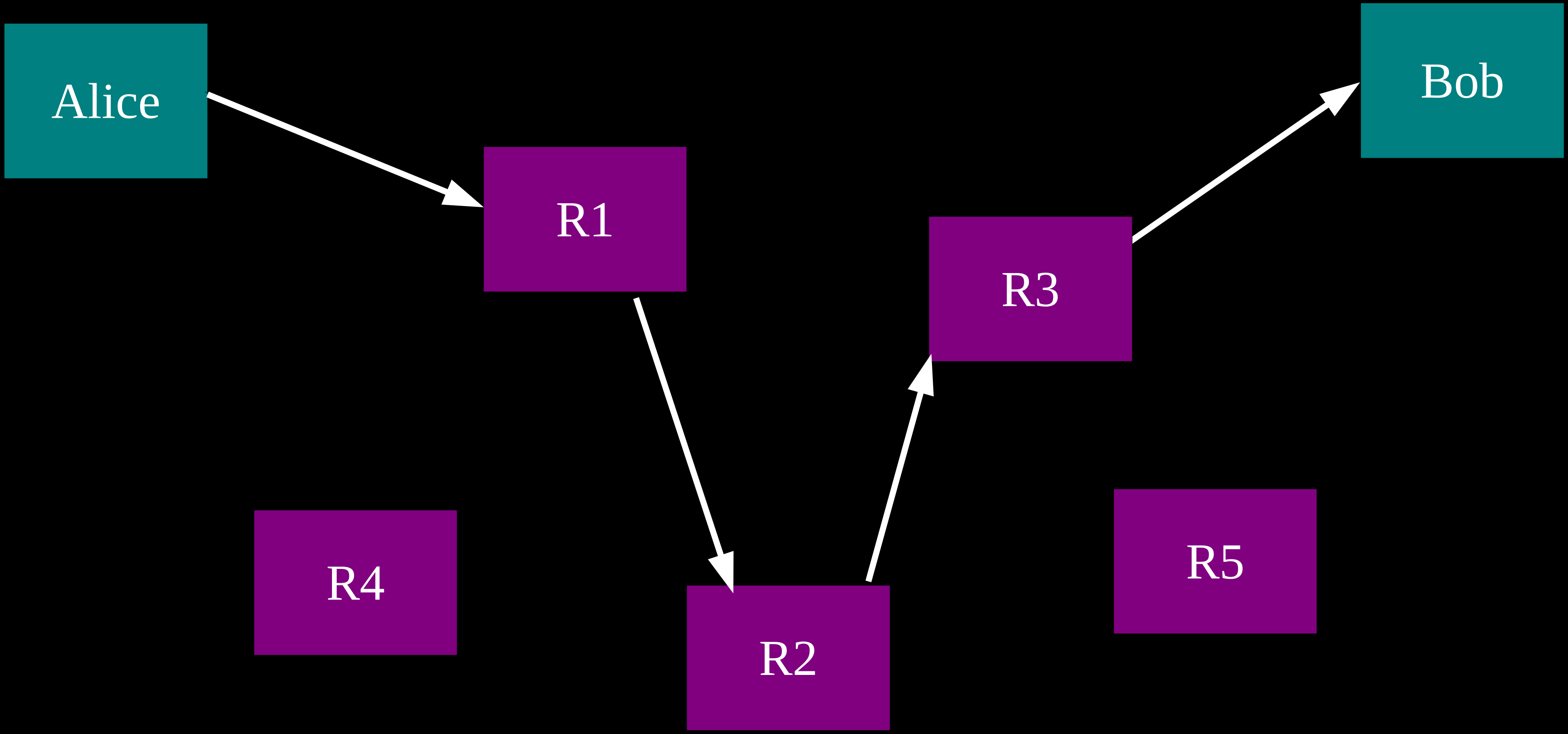


... or a single point of bypass.

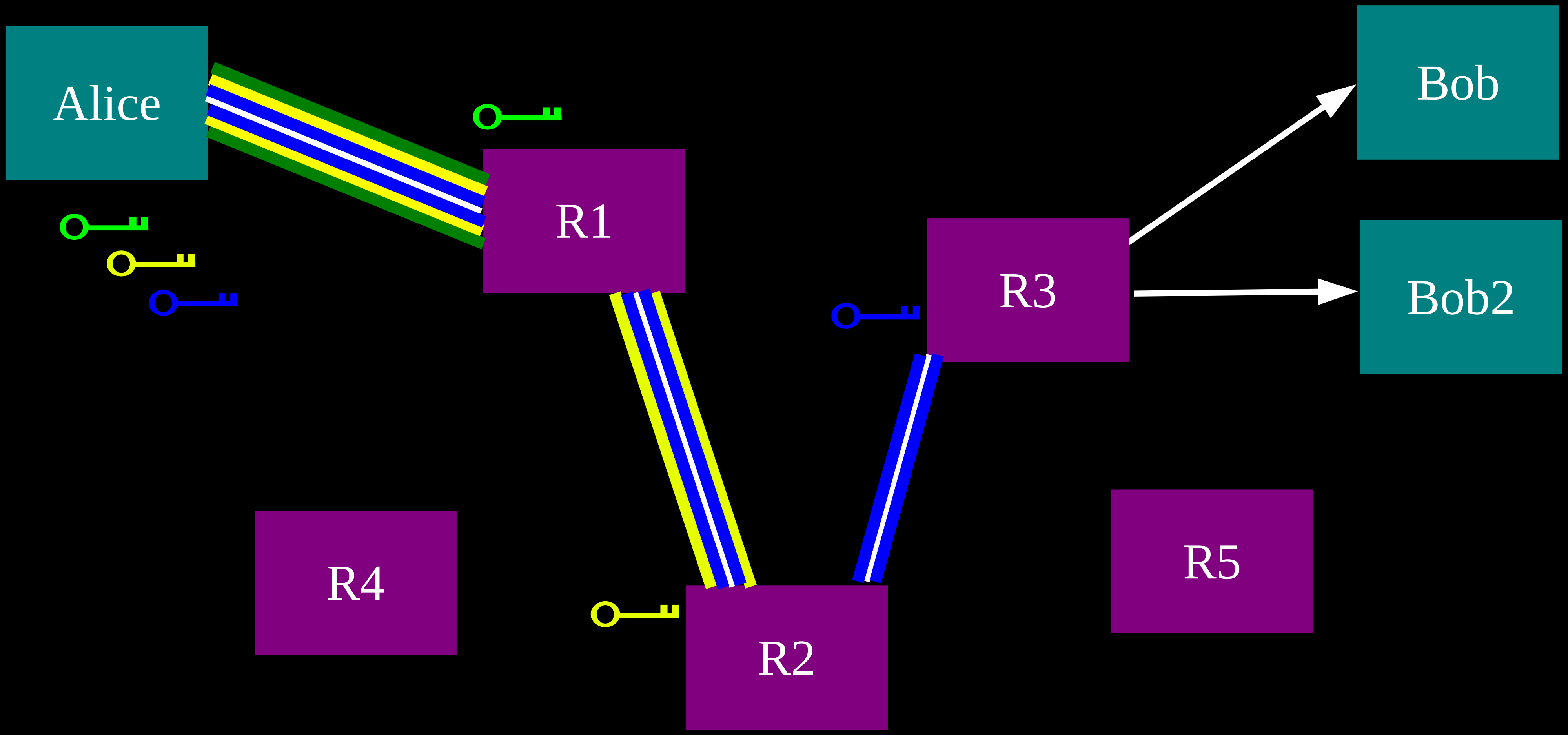


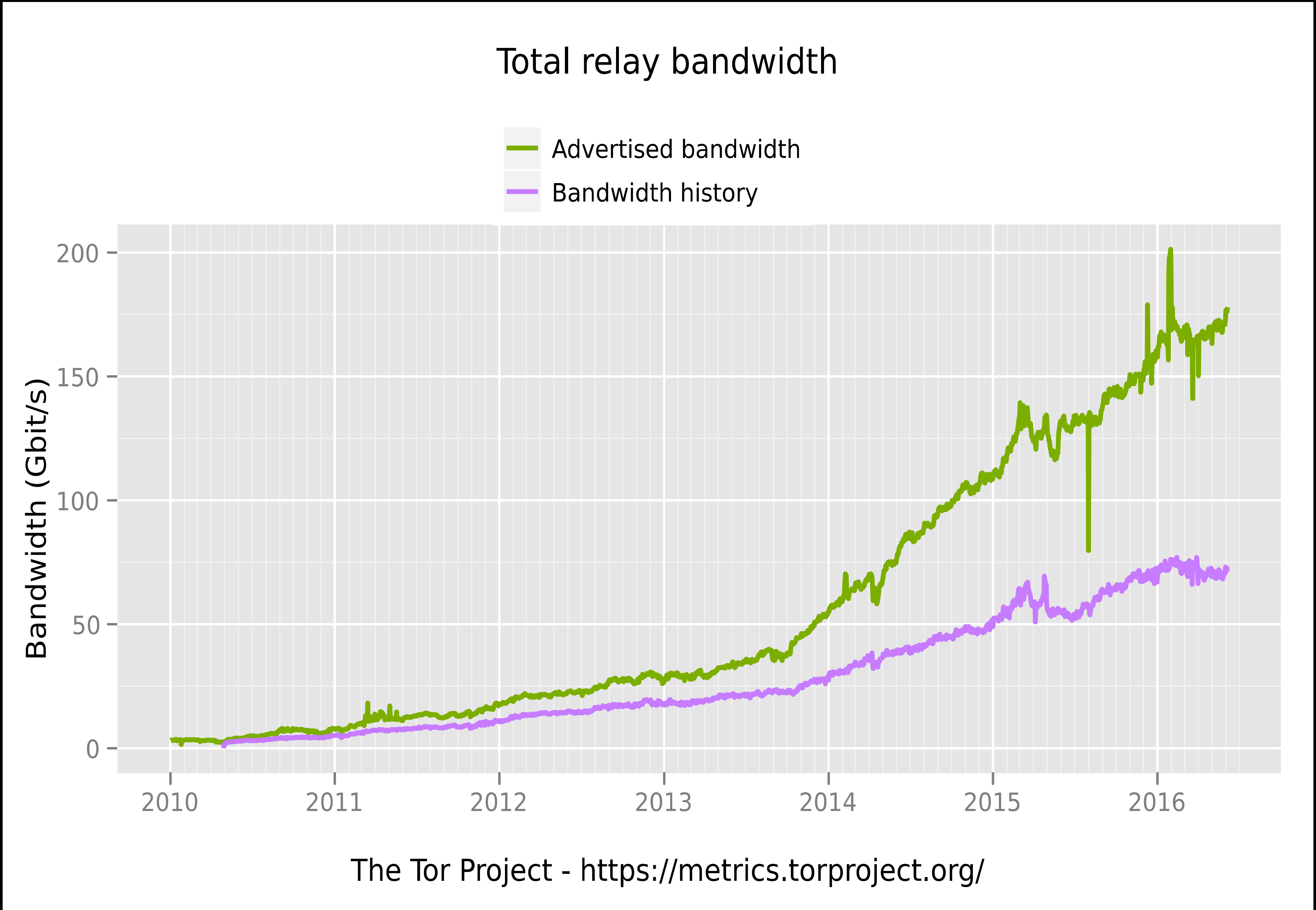
Timing analysis bridges all connections through relay ⇒ An attractive fat target

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



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



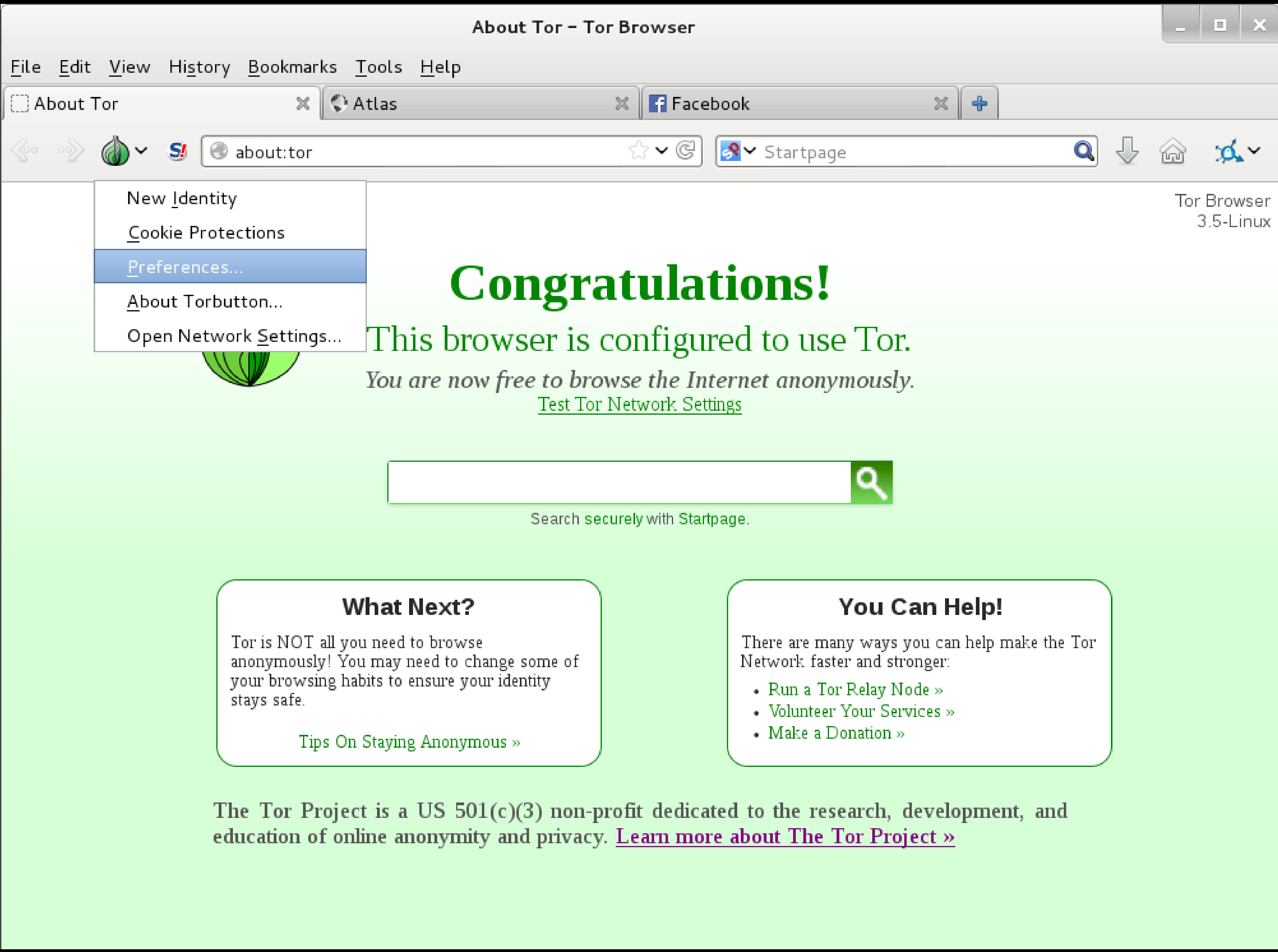


Total relay bandwidth

The Tor Project - https://metrics.torproject.org/

Tor's safety comes from diversity

- #1: Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation. (Research problem: measuring diversity over time)
- #2: Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.



Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

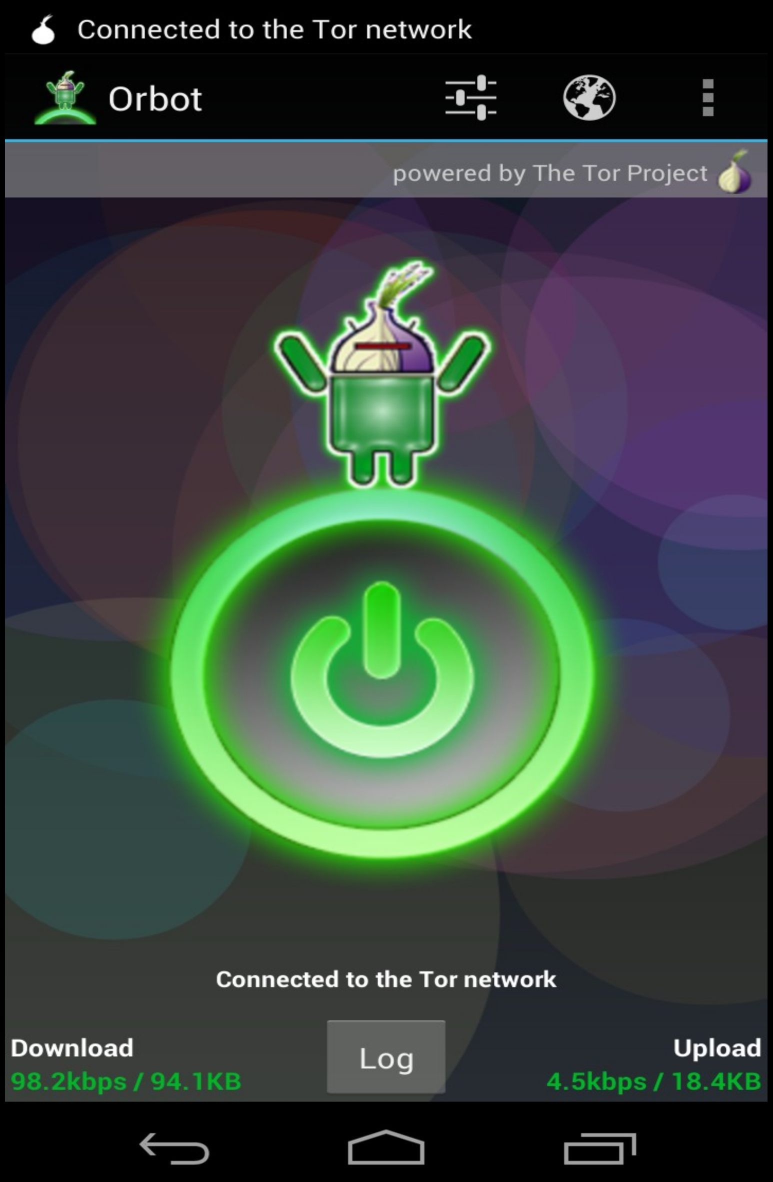
You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

Orbot



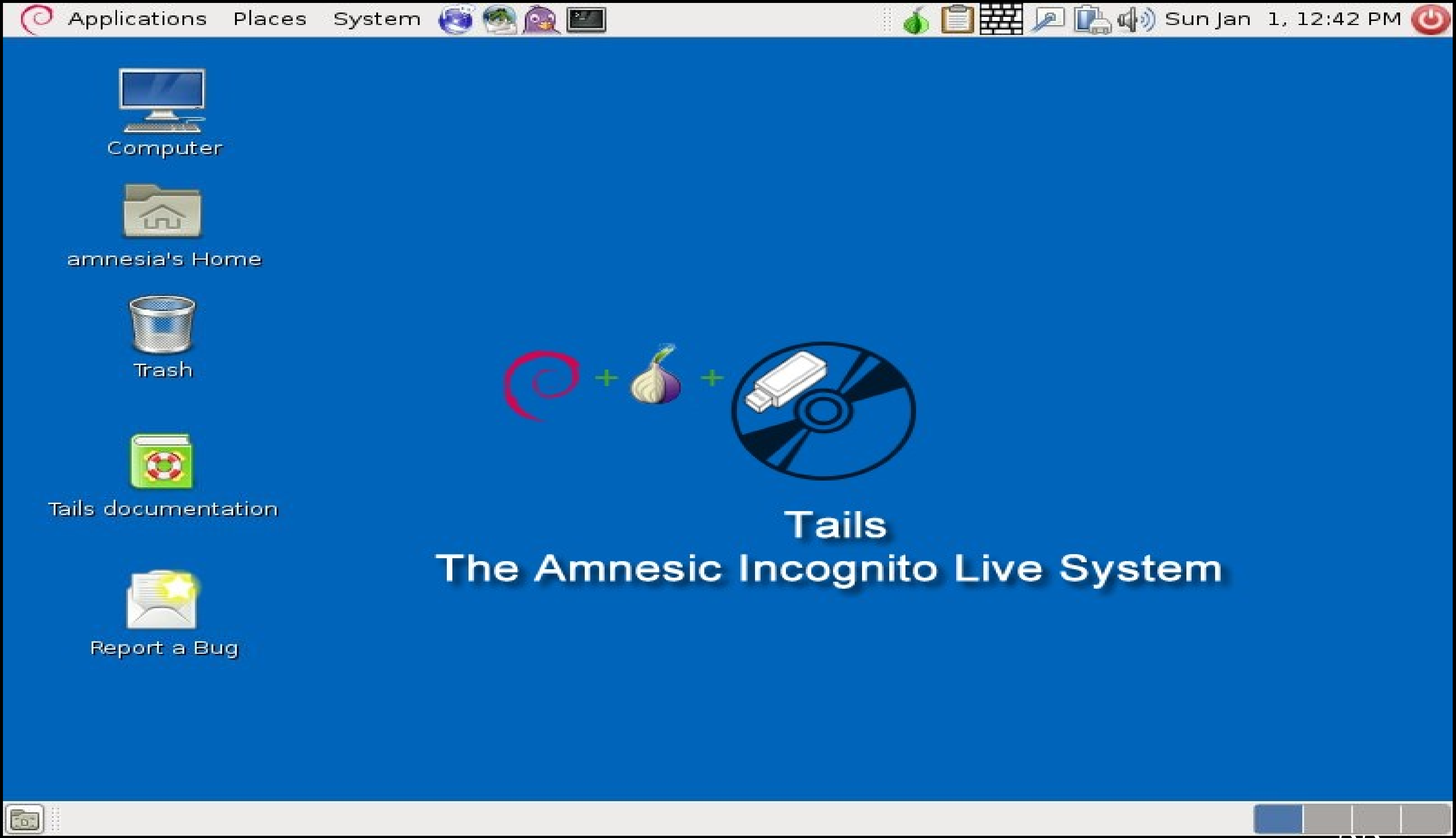
Connected to the Tor network

Connected to the Tor network

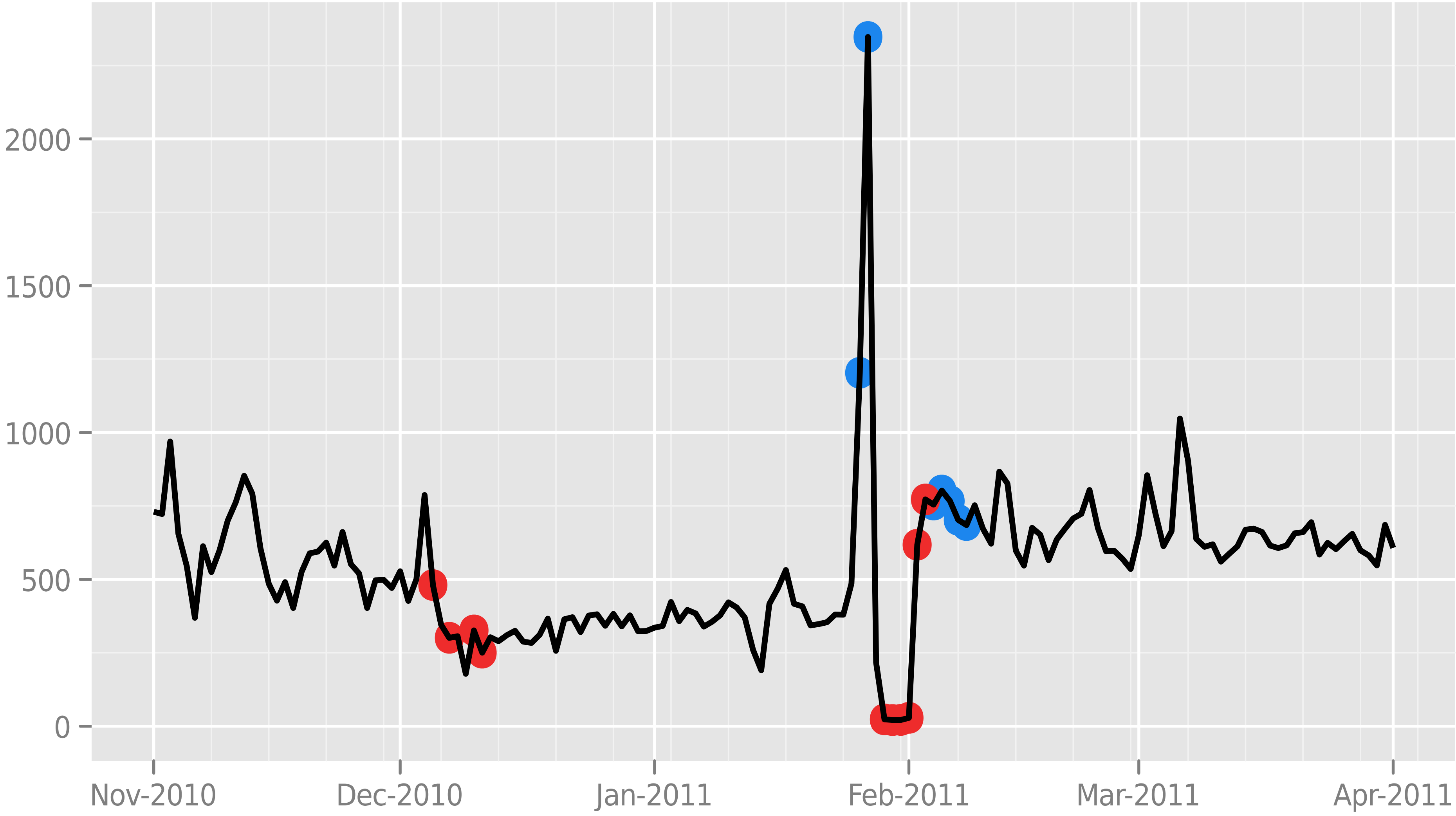
Download
98.2kbps / 94.1KB

Upload
4.5kbps / 18.4KB

Tails LiveCD

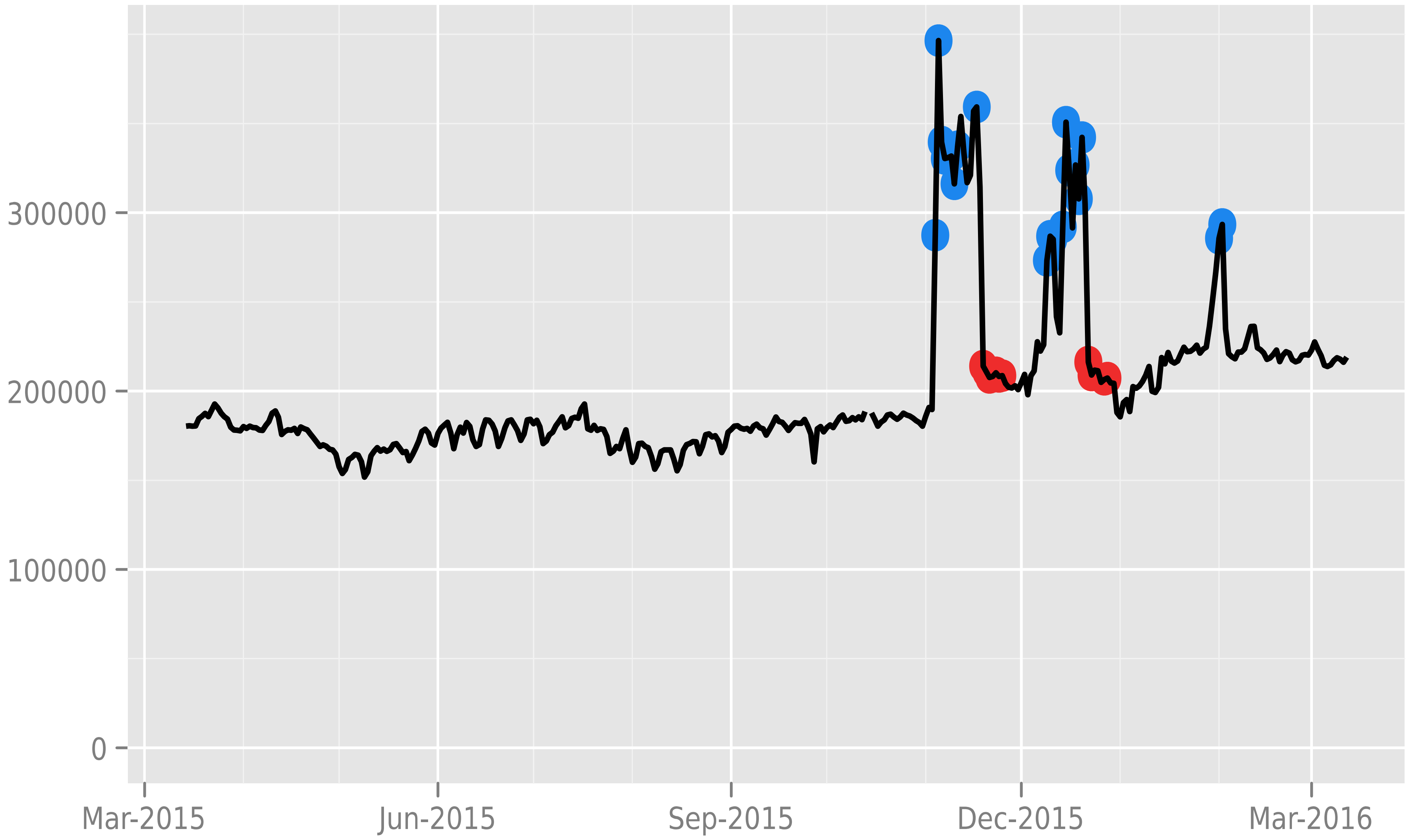


Directly connecting users from Egypt



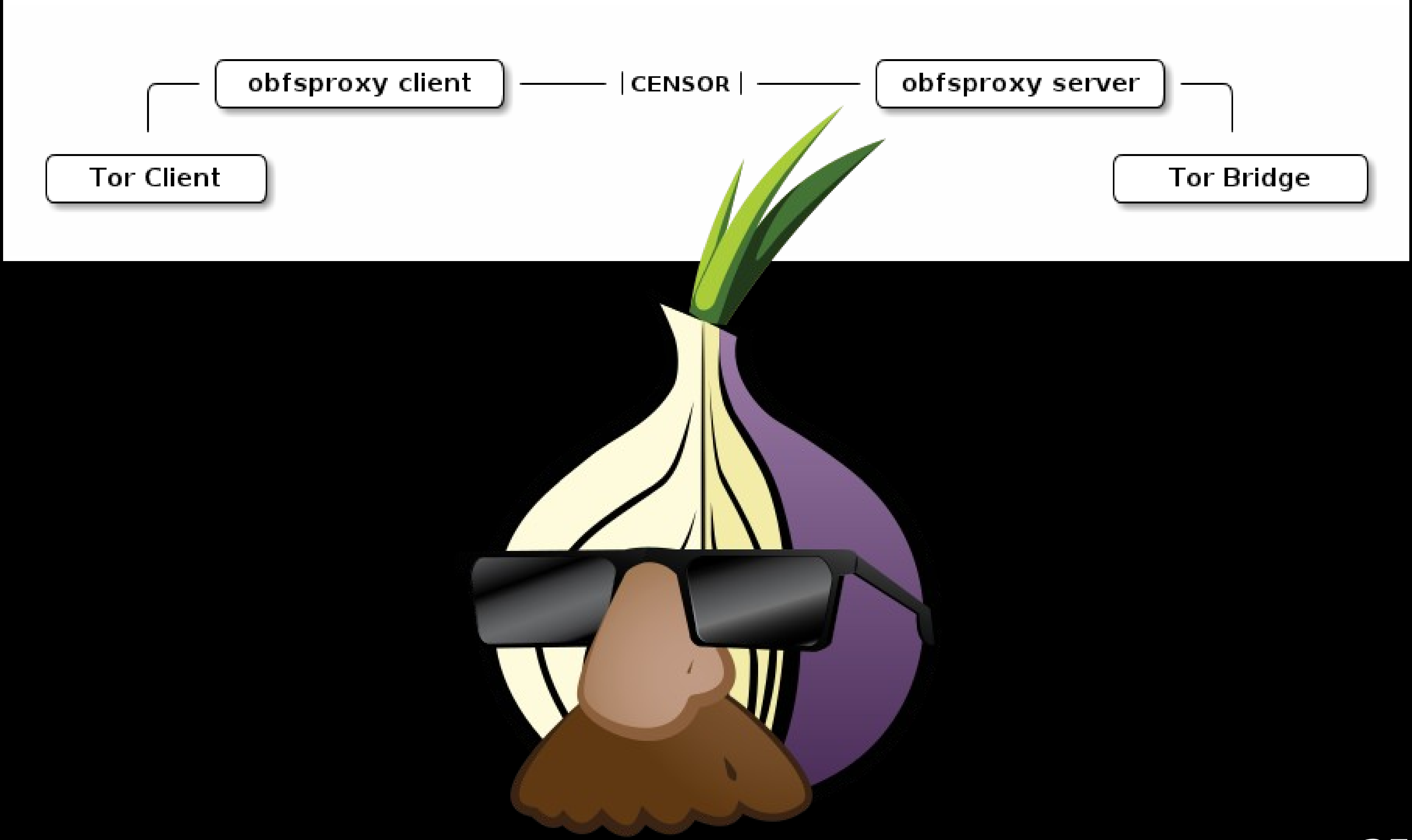
The Tor Project - https://metrics.torproject.org/

Directly connecting users from Russia



The Tor Project - https://metrics.torproject.org/

Pluggable transports



obfsproxy client

|CENSOR|

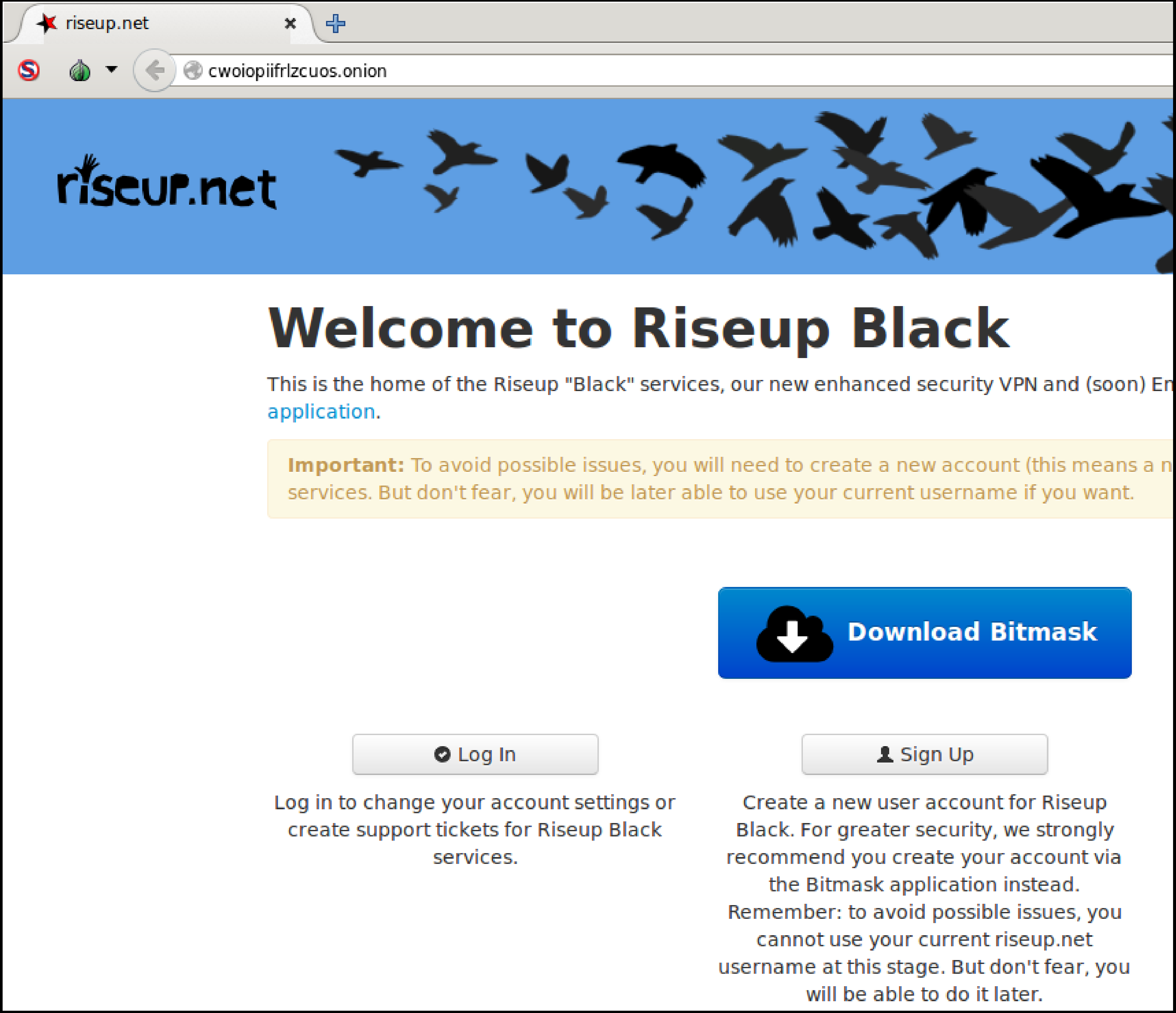
obfsproxy server

Tor Client

Tor Bridge

Pluggable transports

- Flashproxy (Stanford), websocket
- FTEProxy (Portland St), http via regex
- Stegotorus (SRI/CMU), http
- Skypemorph (Waterloo), Skype video
- uProxy (Google), webrtc
- Lantern (BNS), social network based
- ScrambleSuit (Karlstad), obfs-based
- Telex (Michigan/Waterloo), traffic divert



Welcome to Riseup Black

This is the home of the Riseup "Black" services, our new enhanced security VPN and (soon) En application.

Important: To avoid possible issues, you will need to create a new account (this means a n services. But don't fear, you will be later able to use your current username if you want.

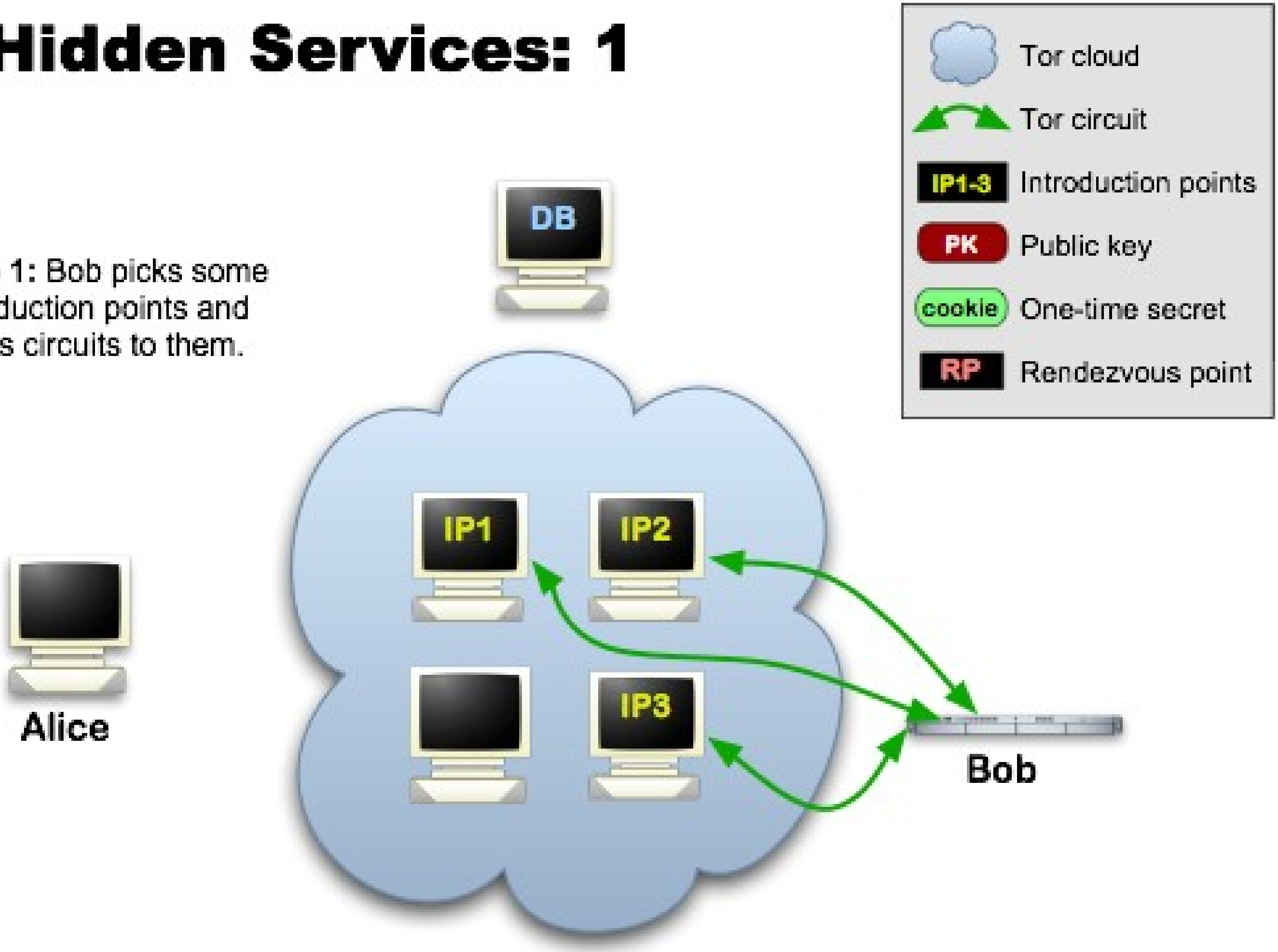
Log in to change your account settings or create support tickets for Riseup Black services.

Create a new user account for Riseup Black. For greater security, we strongly recommend you create your account via the Bitmask application instead. Remember: to avoid possible issues, you cannot use your current riseup.net username at this stage. But don't fear, you will be able to do it later.

Hidden Services

- The ".onion" addresses
  - 16 characters long (base32)
  - E.g: *nzh3fv6jc6jskki3.onion*
- Client **and** Server hide their location
- Can be used for various kinds of TCP traffic
- Everything stays **inside** the Tor network

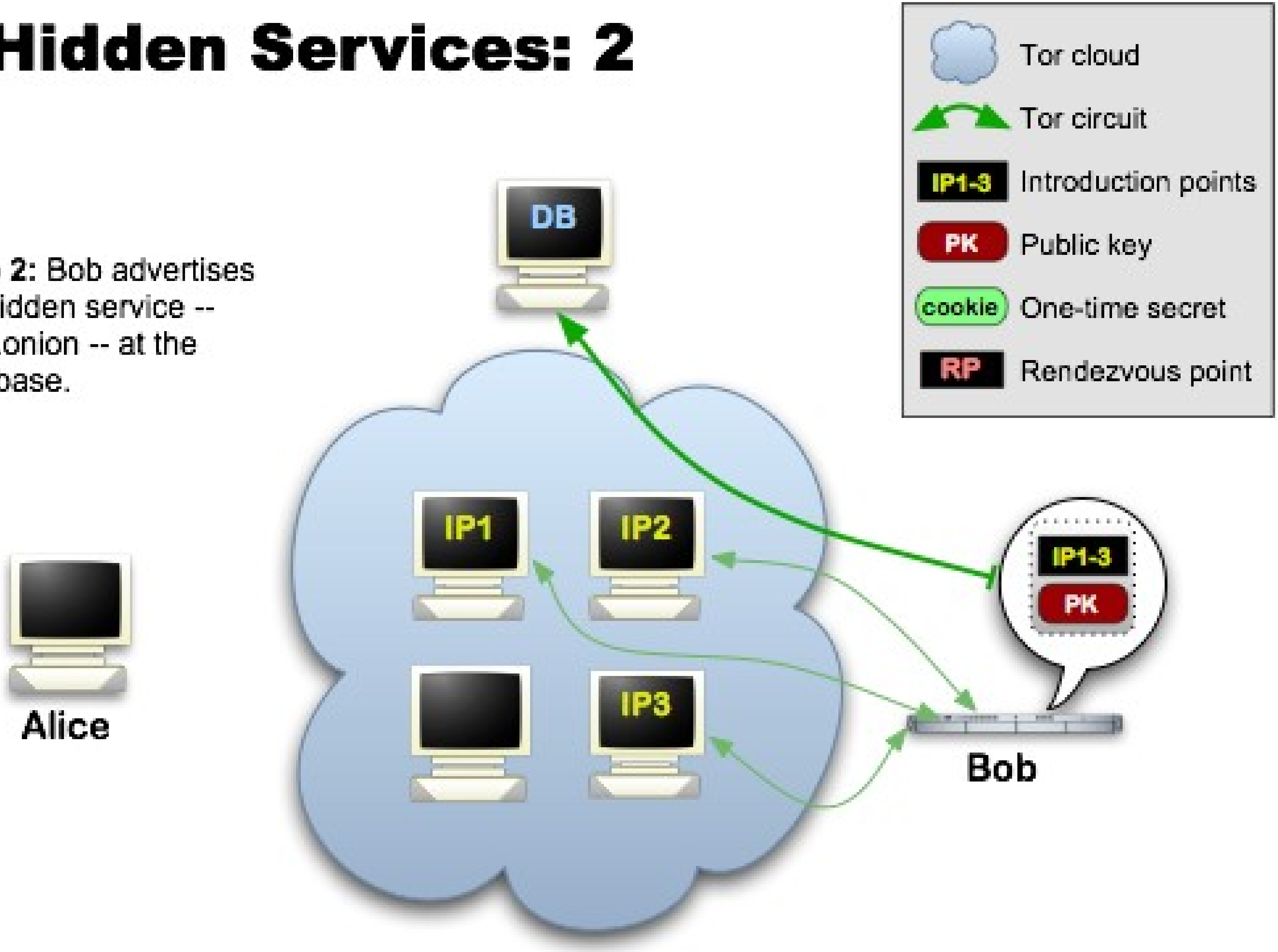
Tor Hidden Services: 1



Step 1: Bob picks some introduction points and builds circuits to them.

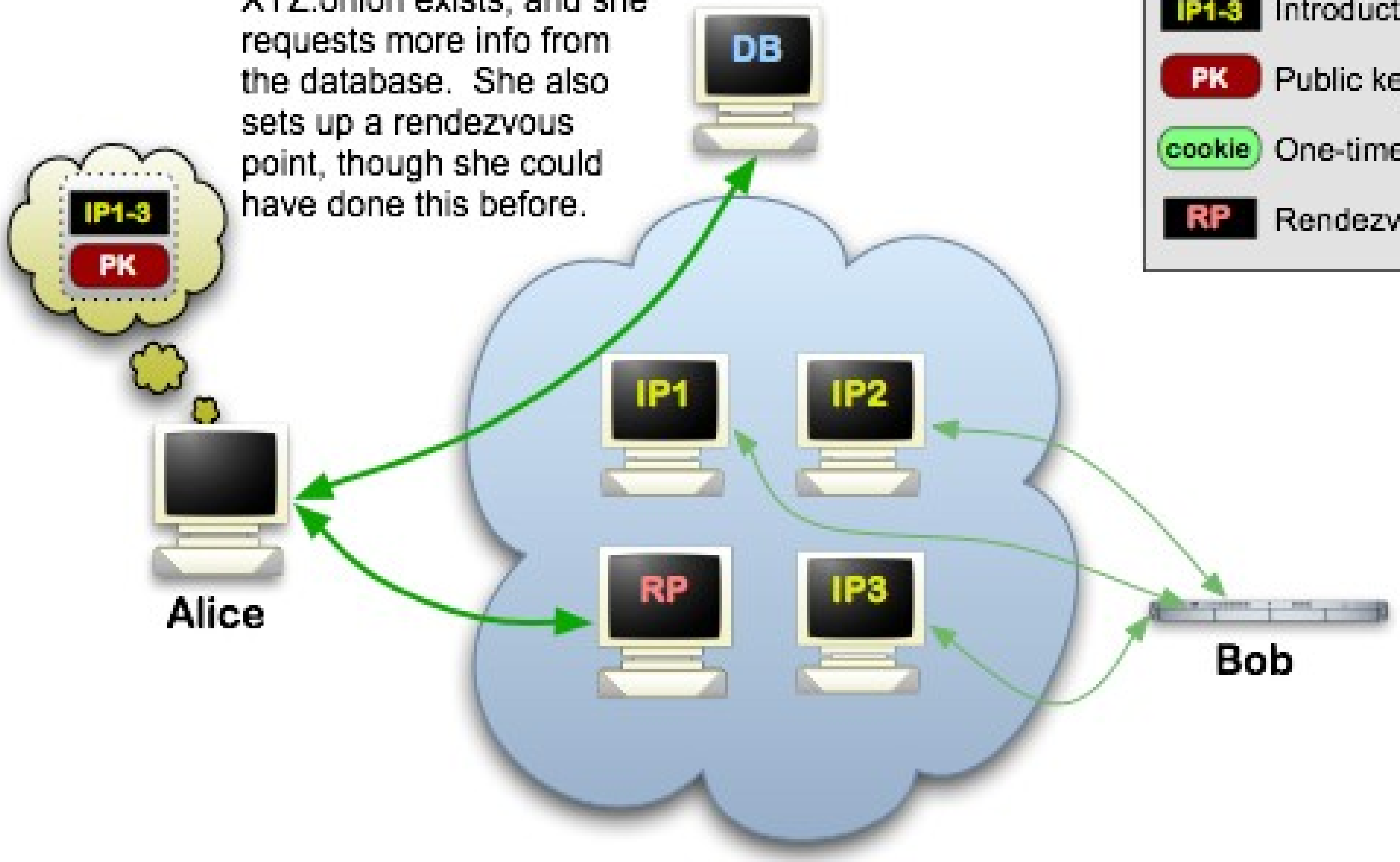
Tor Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



Tor Hidden Services: 3

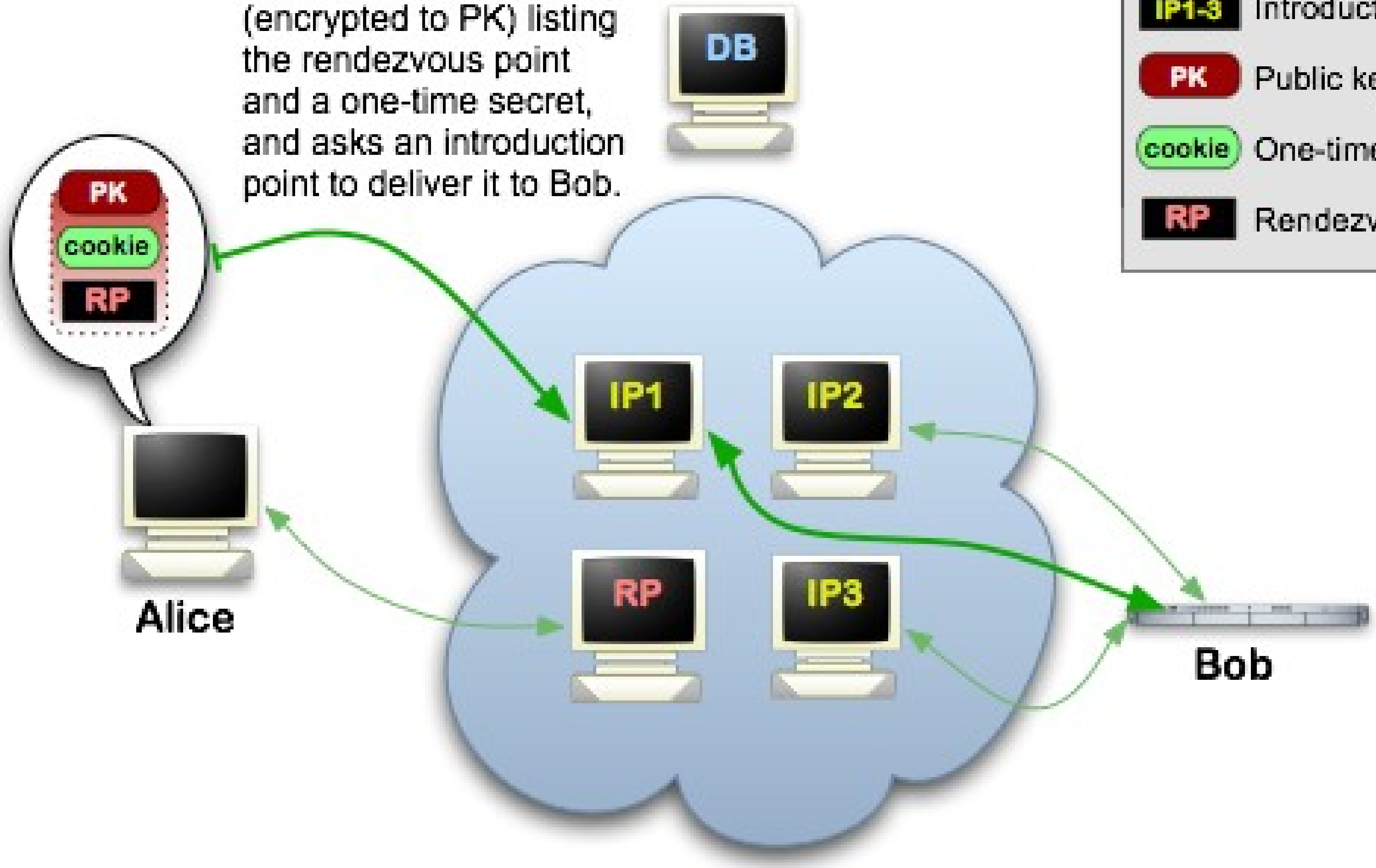
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



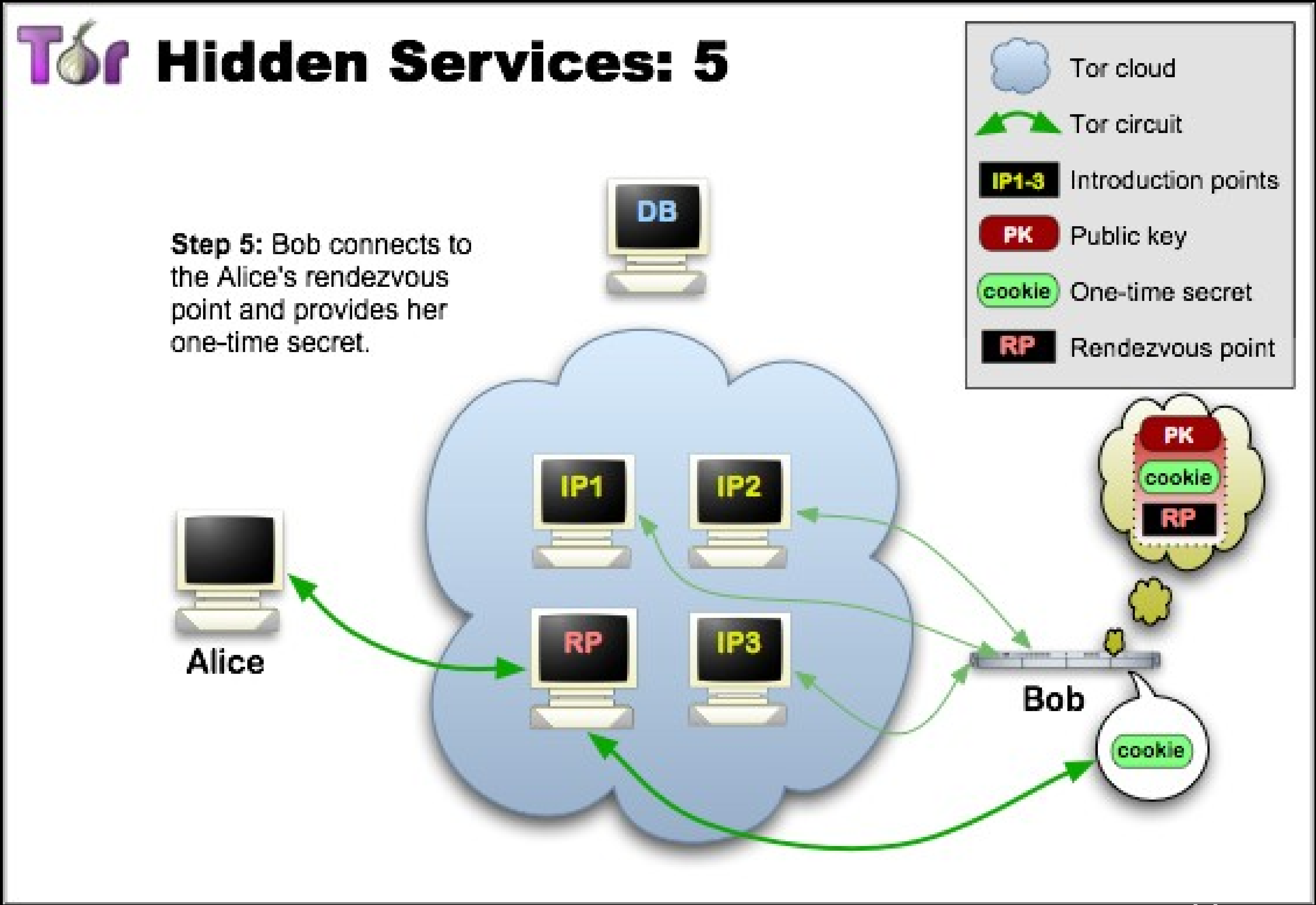
- Tor cloud
- Tor circuit
- IP1-3 Introduction points
- PK Public key
- cookie One-time secret
- RP Rendezvous point

Tor Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



- Tor cloud
- Tor circuit
- IP1-3 Introduction points
- PK Public key
- cookie One-time secret
- RP Rendezvous point



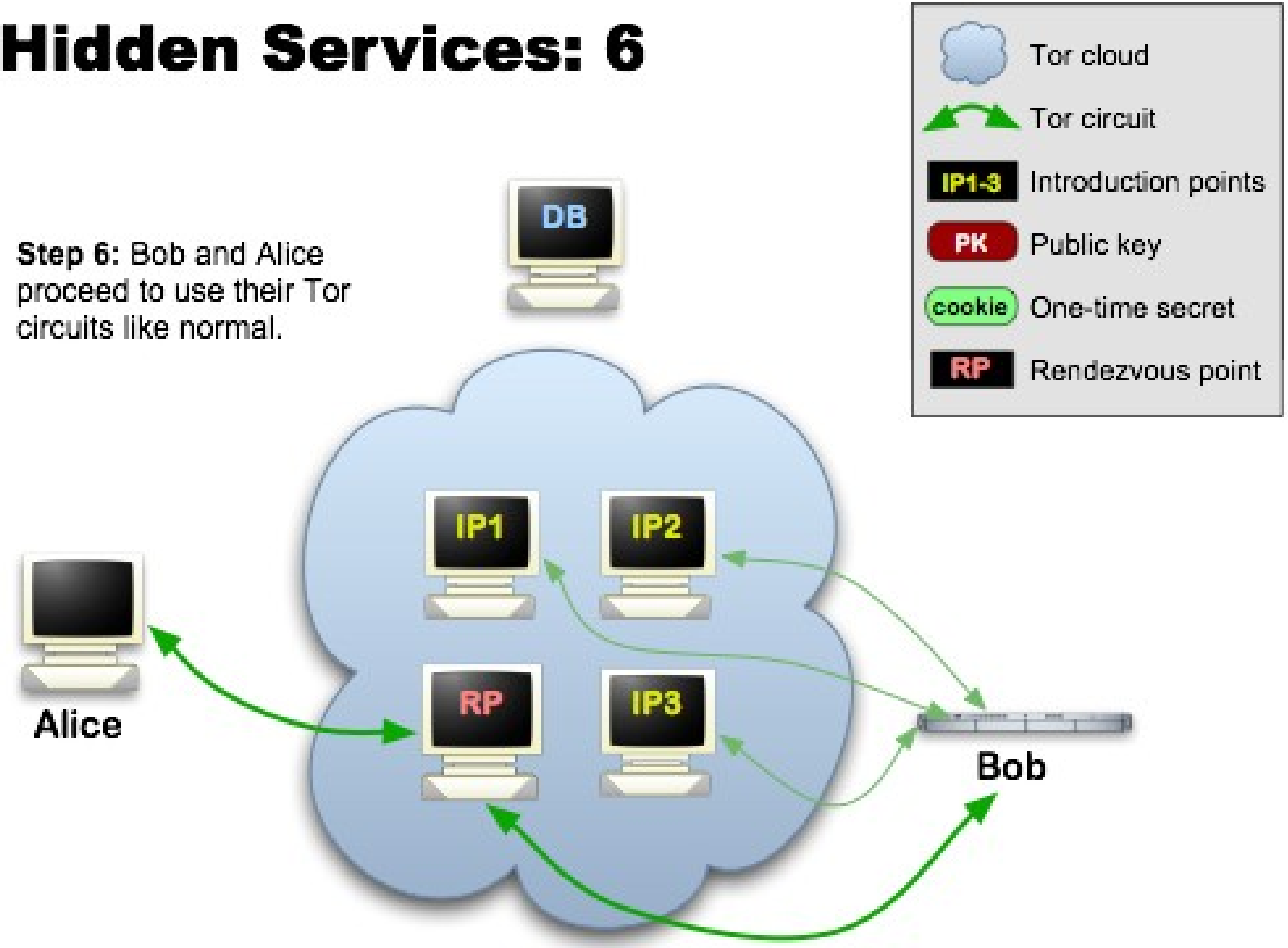
Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.

- Tor cloud
- Tor circuit
- IP1-3 Introduction points
- PK Public key
- cookie One-time secret
- RP Rendezvous point

Tor Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



Onion Service Properties

- Self authenticated
  (self-verifying?)
- End-to-end encrypted
- NAT punching
- Limited surface area

Takeaways

More variation in onion services than people think.

Still a **tiny** fraction of overall Tor traffic.

Upcoming technical work to make them **harder / better / stronger / faster**.

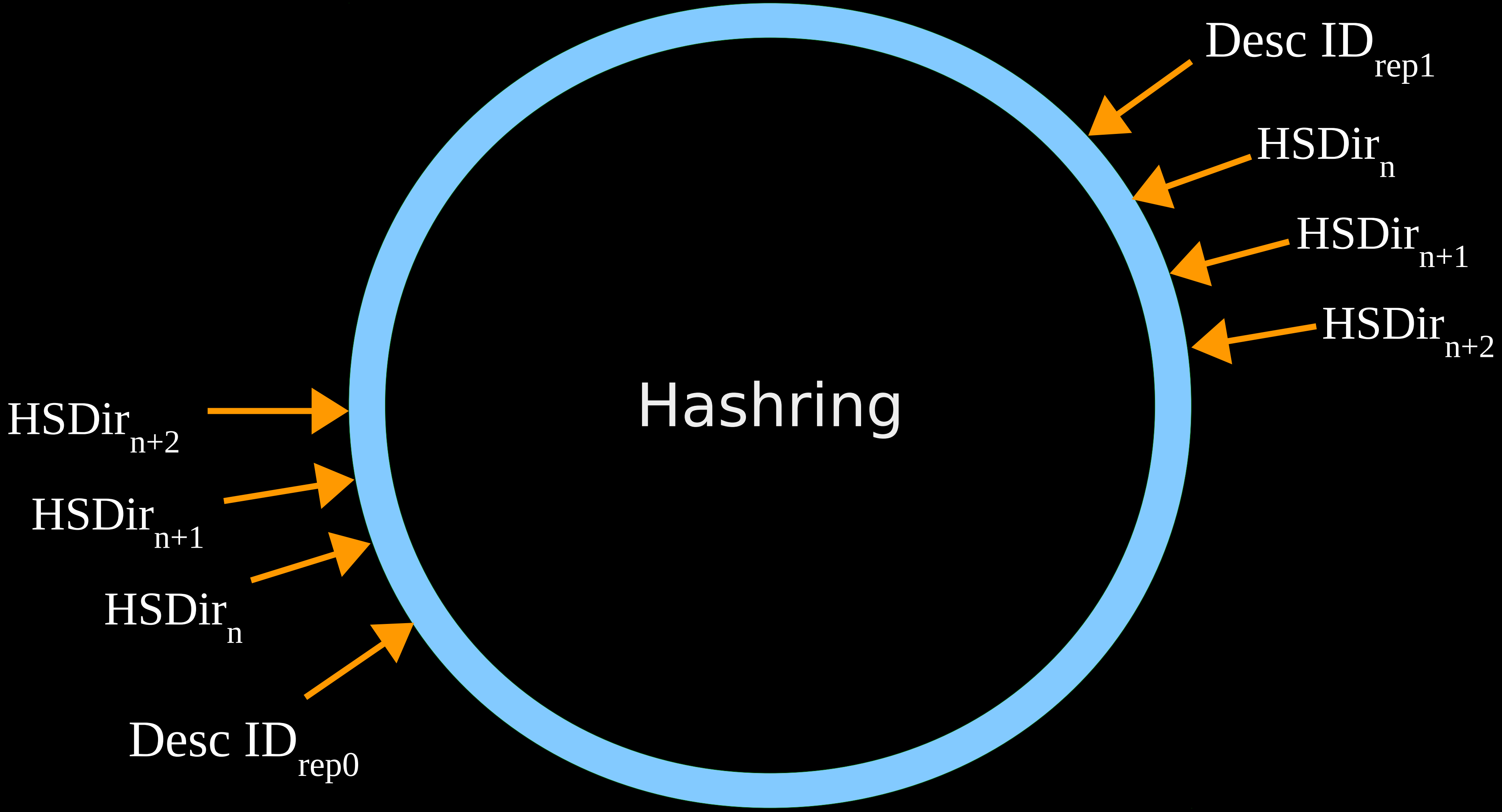
Please **deploy** an onion address for your website/service

Current Security Problems

- Onion identity keys are **too short**!
- You can choose relay identity keys to **target** a particular onion service
- You can run relays to **harvest** onion addresses
- **Sybil** attacks remain an issue for Tor in general
- Guard **discovery** attack (proposal 247)
- Website **fingerprinting** for onion services?

HS Directory

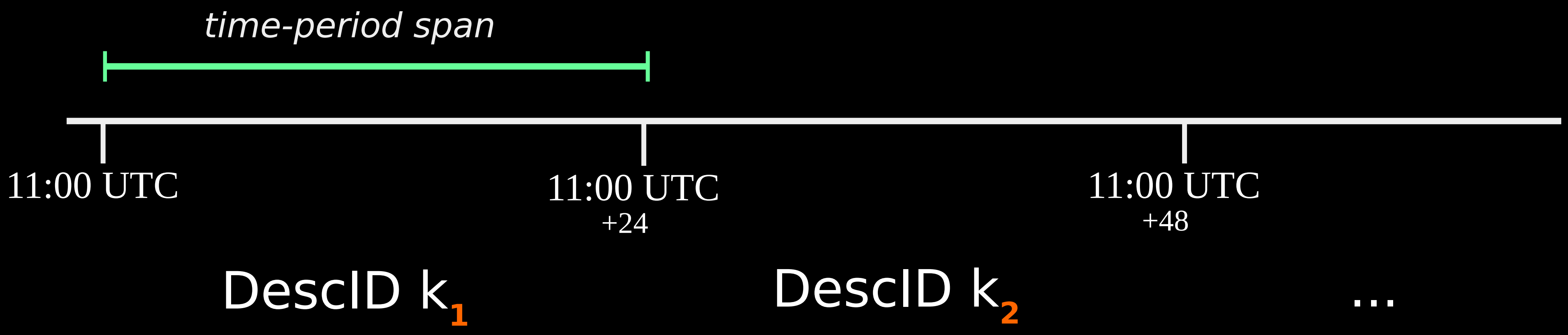
Desc ID = H(onion-address | H(time-period | descriptor-cookie | replica))



HSDir Predictibility

Desc ID = H(onion-address |
H(**time-period** | descriptor-cookie | replica))

🟦 Invariant



time-period span

11:00 UTC

11:00 UTC +24

11:00 UTC +48

DescID k_1

DescID k_2

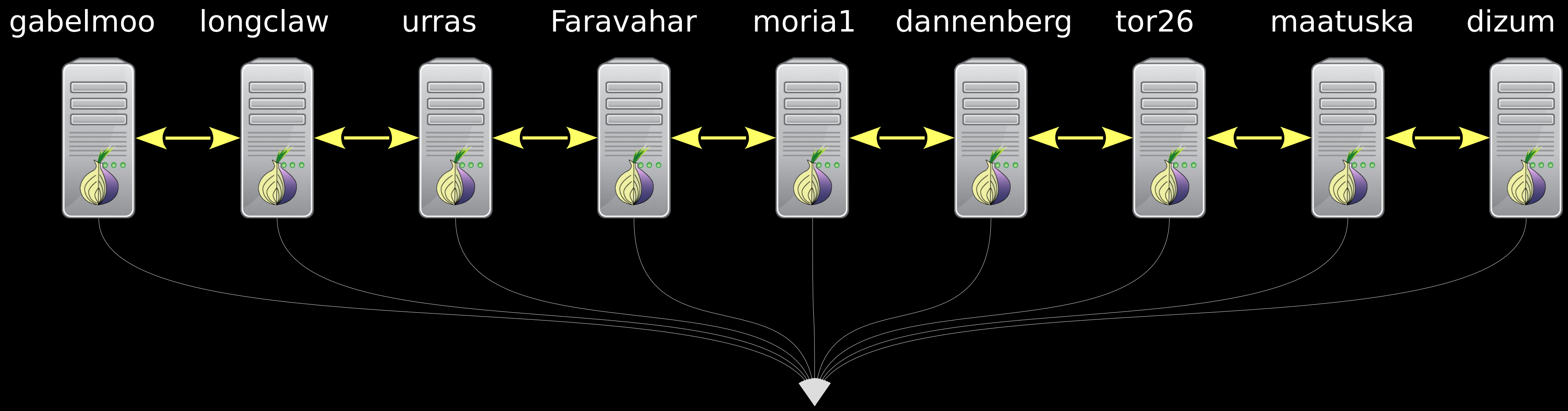
...

Shared Randomness

Proposal 250

Desc ID = H(onion-address |
H(**time-period** | **random-value** | descriptor-cookie | replica))

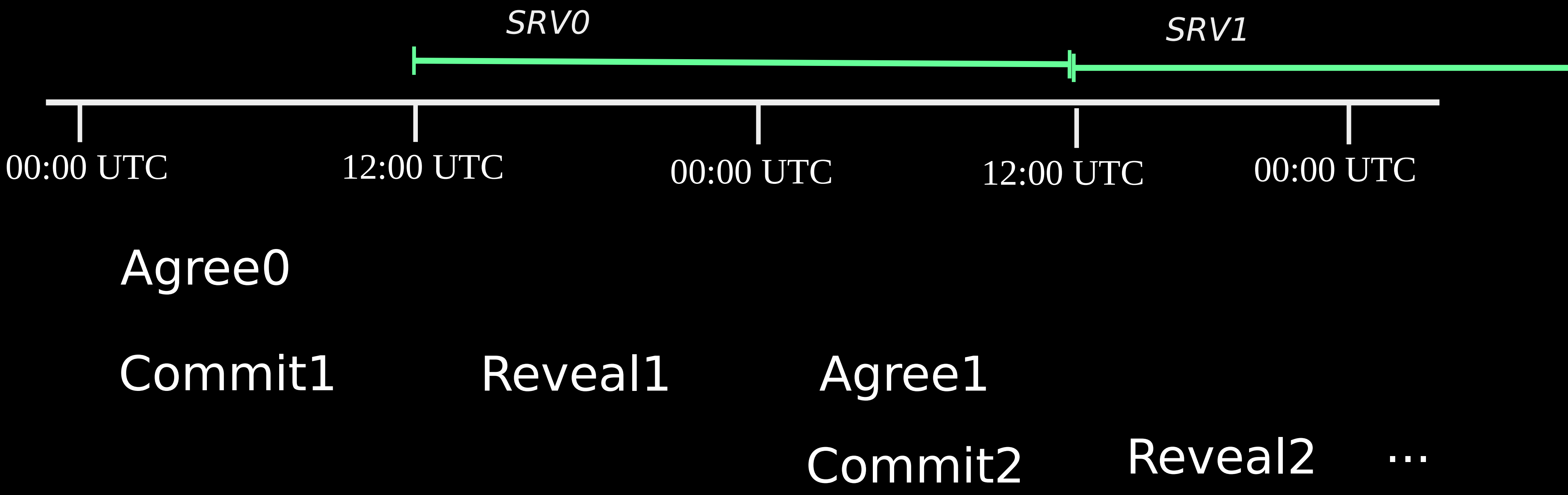
🟦 Invariant



random-value

(new every 24h)

Shared-Random-Value phases



SRV0

SRV1

00:00 UTC

12:00 UTC

00:00 UTC

12:00 UTC

00:00 UTC

Agree0

Commit1 Reveal1 Agree1

Commit2 Reveal2 ...

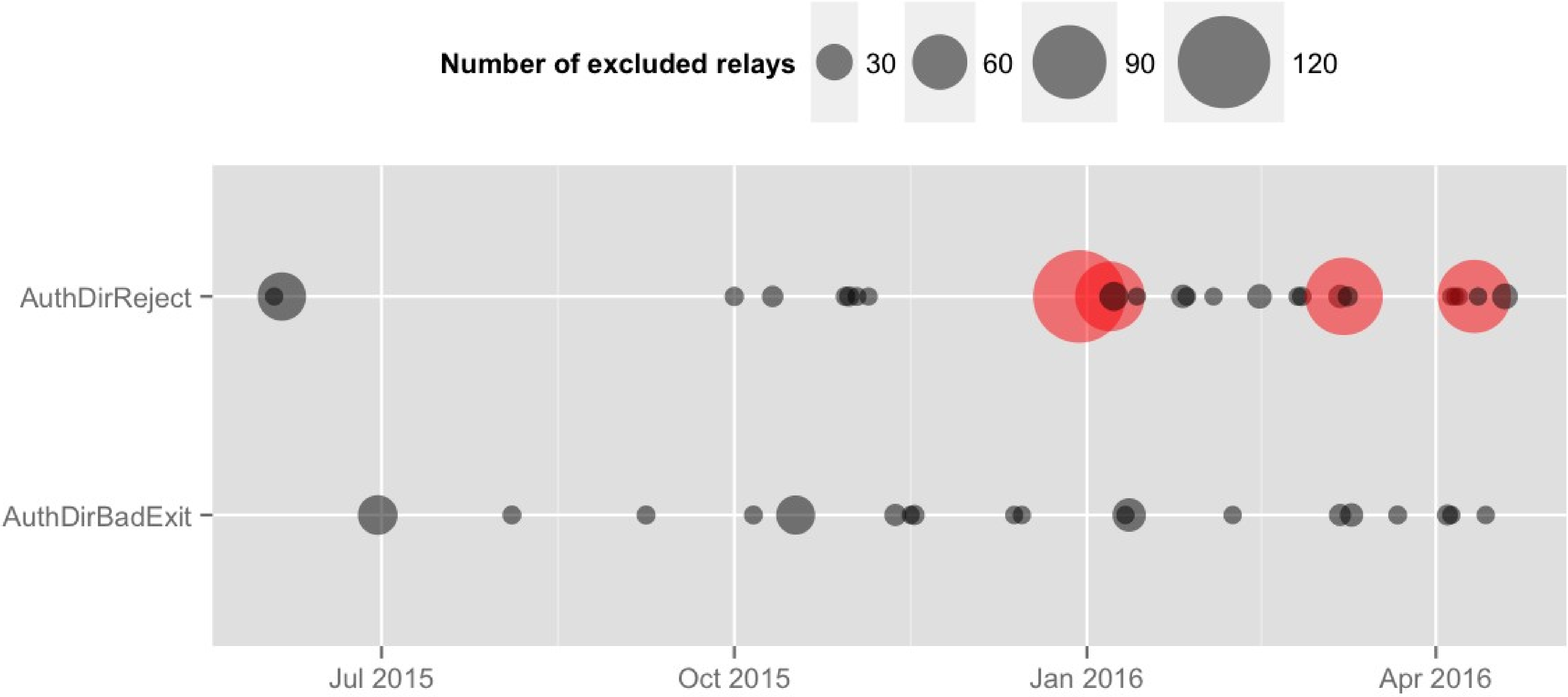
Guidelines for doing your Tor research safely/ethically

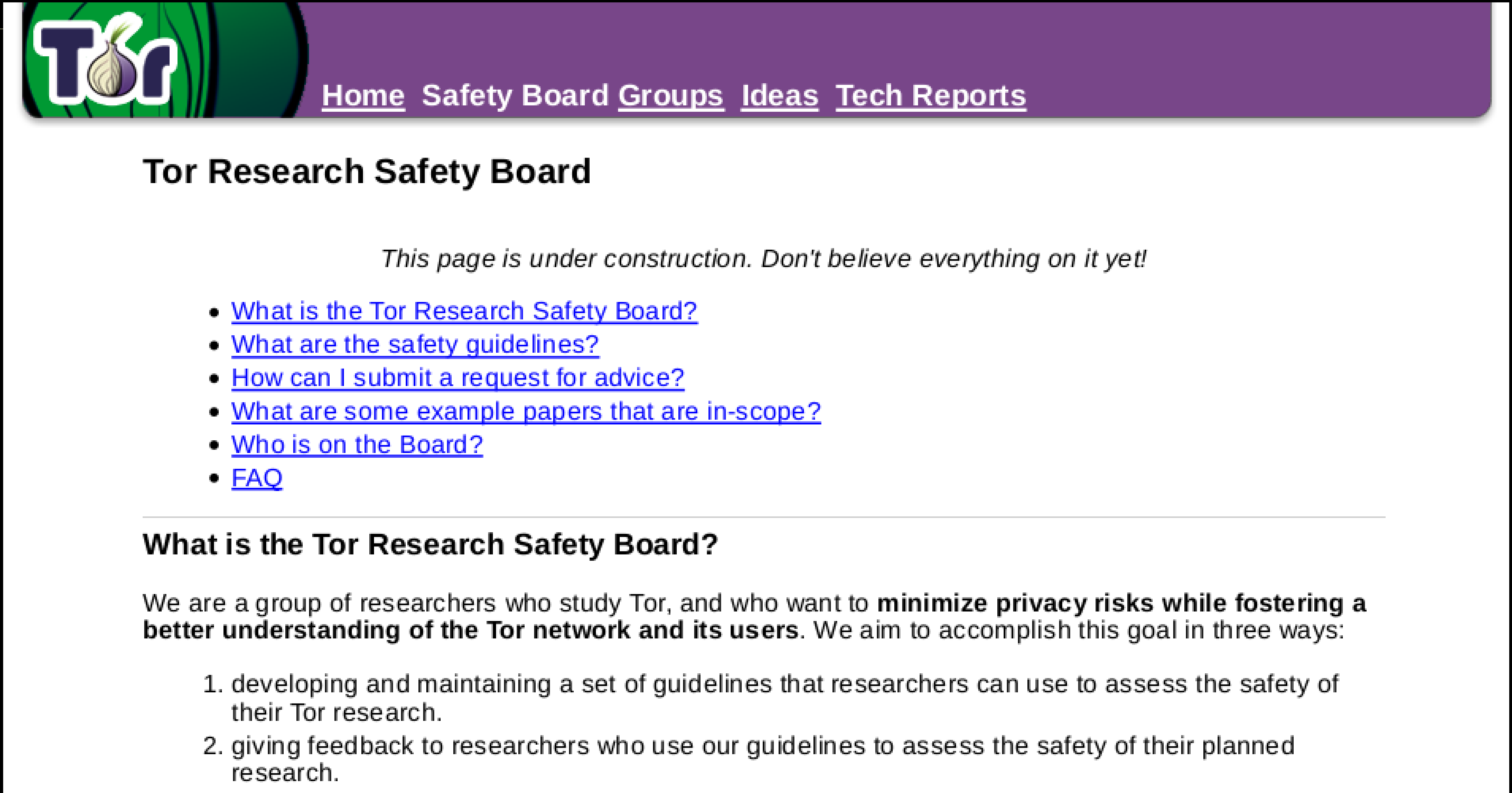
- Try to attack only yourself / your own traffic
- Only collect data that is **acceptable** to make public
- Don't collect data you don't need (minimization)
- Limit the granularity of data (e.g. add noise)
- Describe benefits and risks, and explain why benefits outweigh risks
- Consider auxiliary data when assessing the risks
- Use a Test network whenever possible

Tricky Edge Cases

Onion address harvesting

- Get them by googling for .onion? Ok.
- Get them by being Verisign and looking at the root nameservers? Hm. Ok?
- Get them by being Comcast and looking at your DNS logs? Hm. Ok?
- Get them by running a Tor relay, getting the HSDir flag, and logging what you see? Hm. Not Ok.


Number of excluded relays
30
60
90
120
AuthDirReject
AuthDirBadExit
Jul 2015
Oct 2015
Jan 2016
Apr 2016



Tor Research Safety Board

This page is under construction. Don't believe everything on it yet!

- What is the Tor Research Safety Board?
- What are the safety guidelines?
- How can I submit a request for advice?
- What are some example papers that are in-scope?
- Who is on the Board?
- FAQ

What is the Tor Research Safety Board?

We are a group of researchers who study Tor, and who want to **minimize privacy risks while fostering a better understanding of the Tor network and its users**. We aim to accomplish this goal in three ways:

1. developing and maintaining a set of guidelines that researchers can use to assess the safety of their Tor research.
2. giving feedback to researchers who use our guidelines to assess the safety of their planned research.

Better Crypto

SHA~~1~~ 256
ALL THE THINGS
memegenerator.net

Bigger Onion Address

From 16 characters:

nzh3fv6jc6jskki3.onion

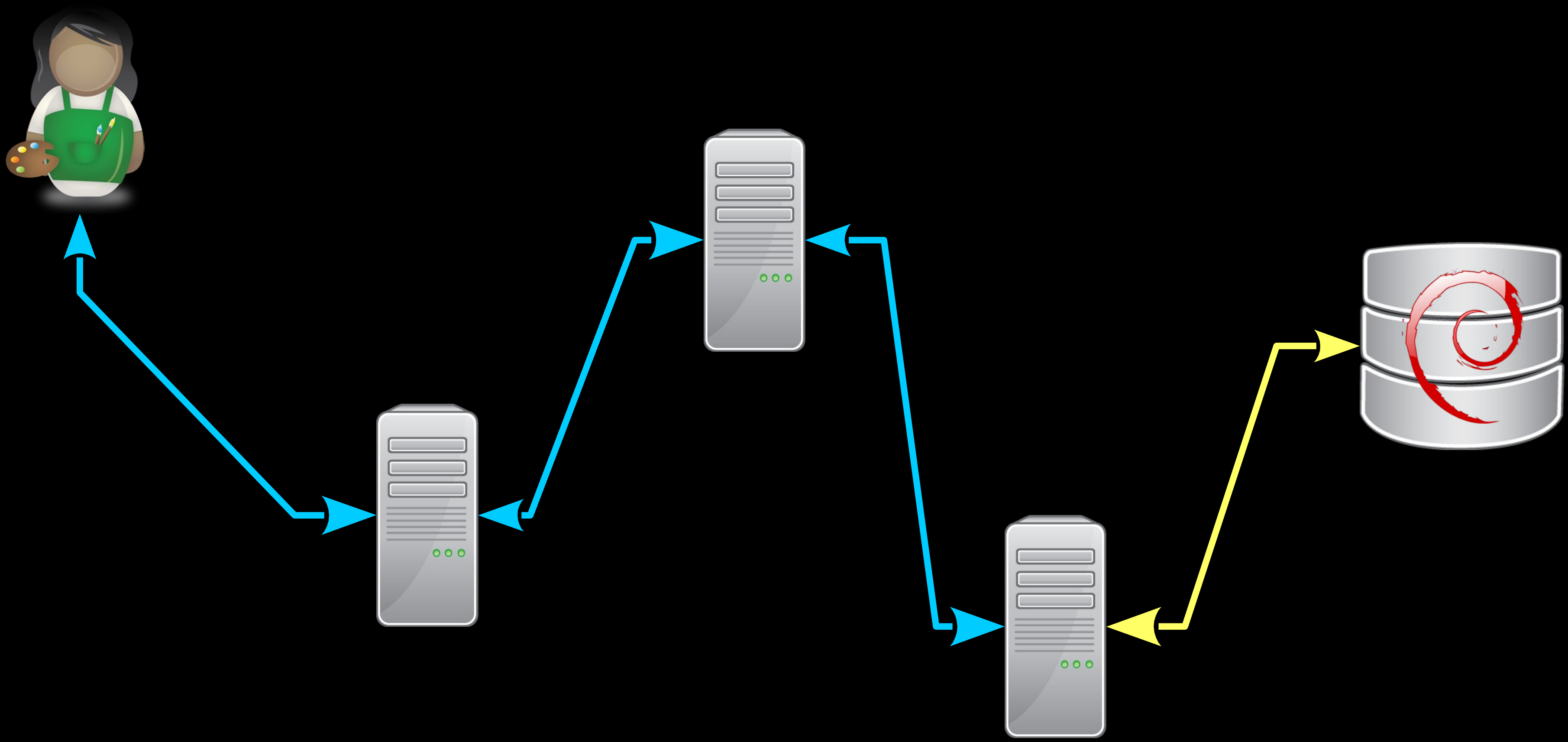
... to 52 characters:

a1uik0w1gmfq3i5ievxdm9ceu27e88g6o7pe0rffdw9jmntwkdsd.onion

(ed25519 public key base32 encoded)

Rendezvous Single Onion Services (RSOS)

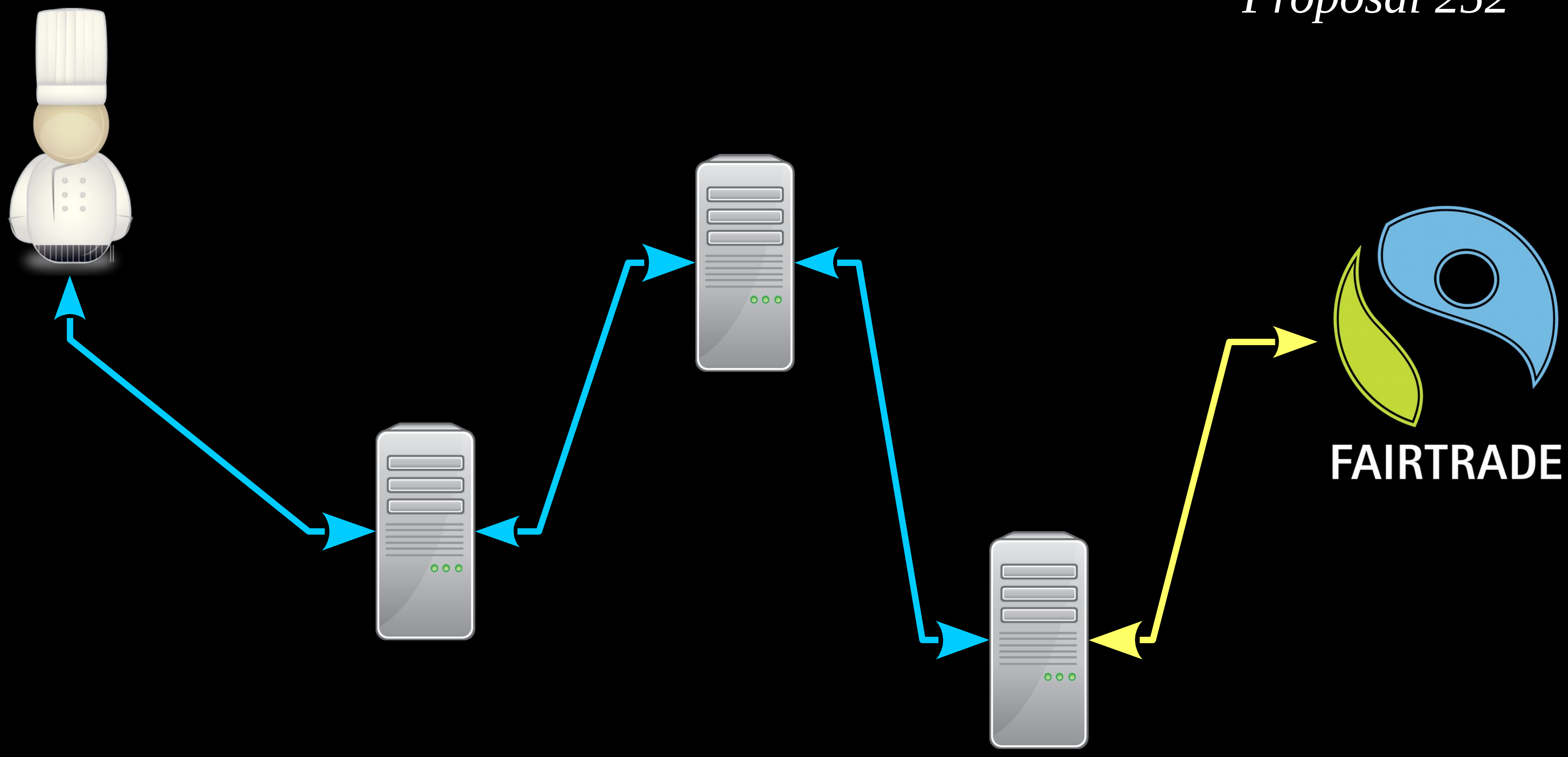
Proposal 260



Rendezvous Point

Single Onion Services (SOS)

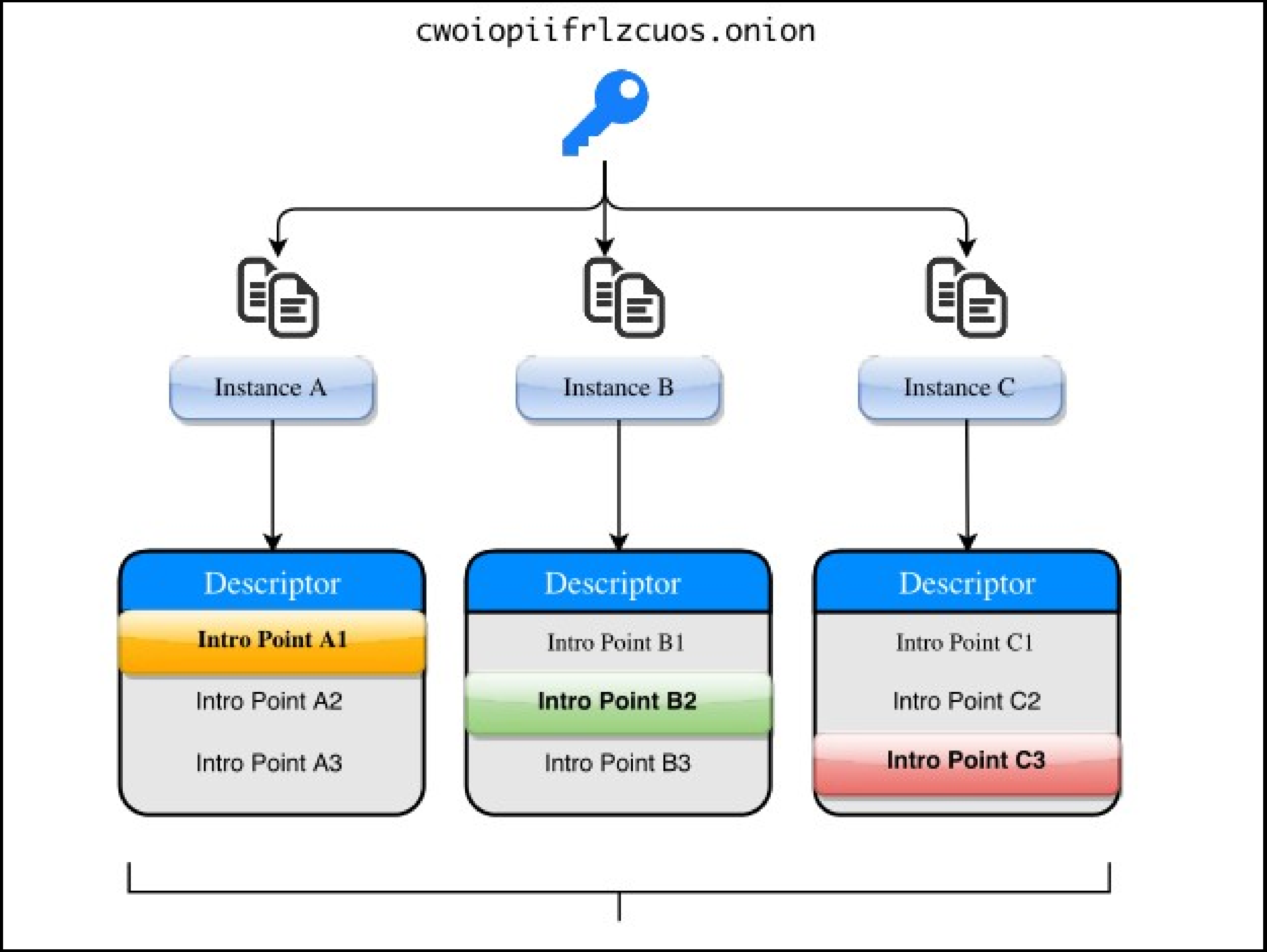
Proposal 252



The circuit is **<u>extended</u>** to the service.
No Introduction nor Rendezvous.

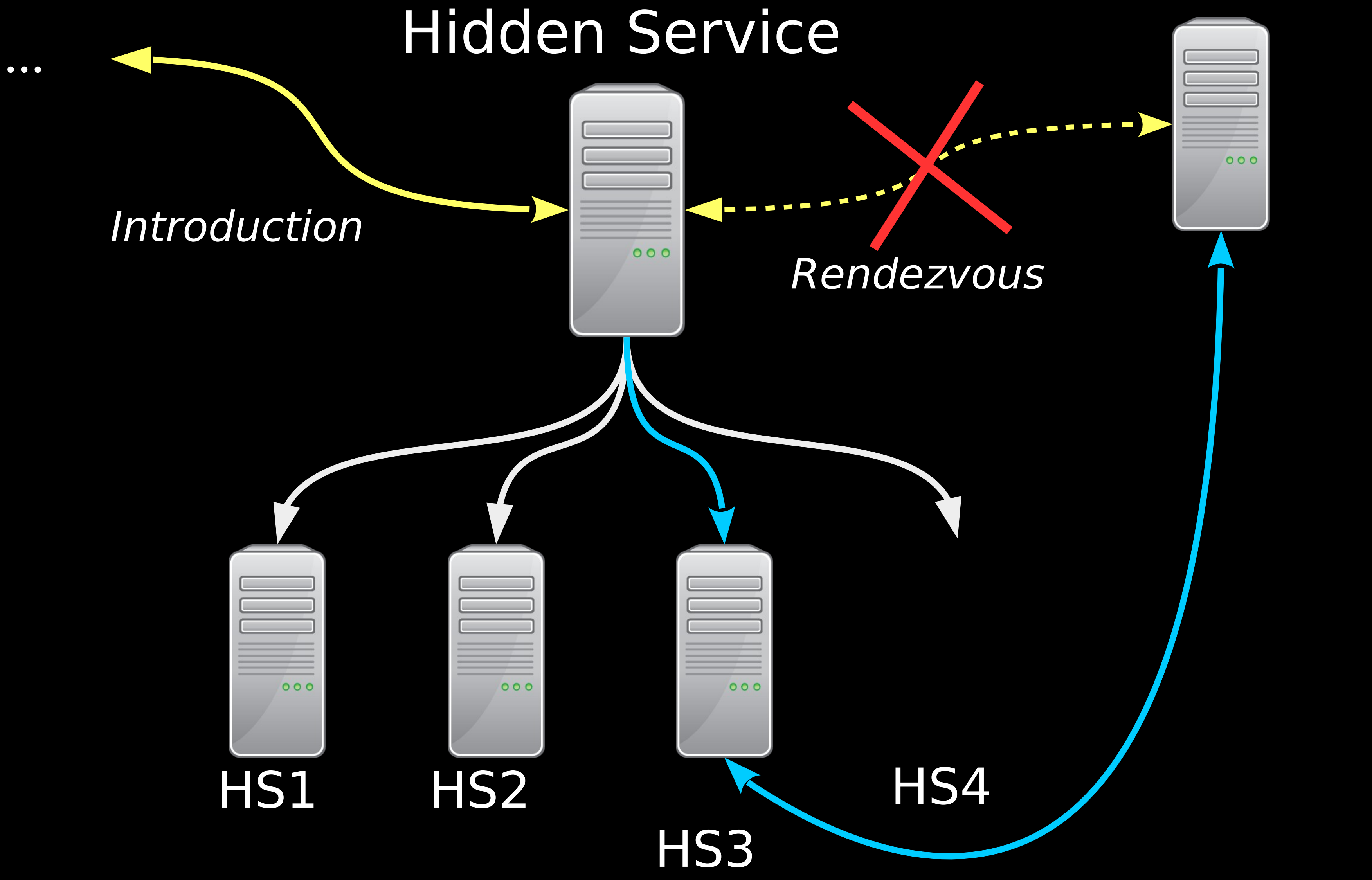
OnionBalance - TSoP

https://onionbalance.readthedocs.org



Load Balancing

Proposal 255

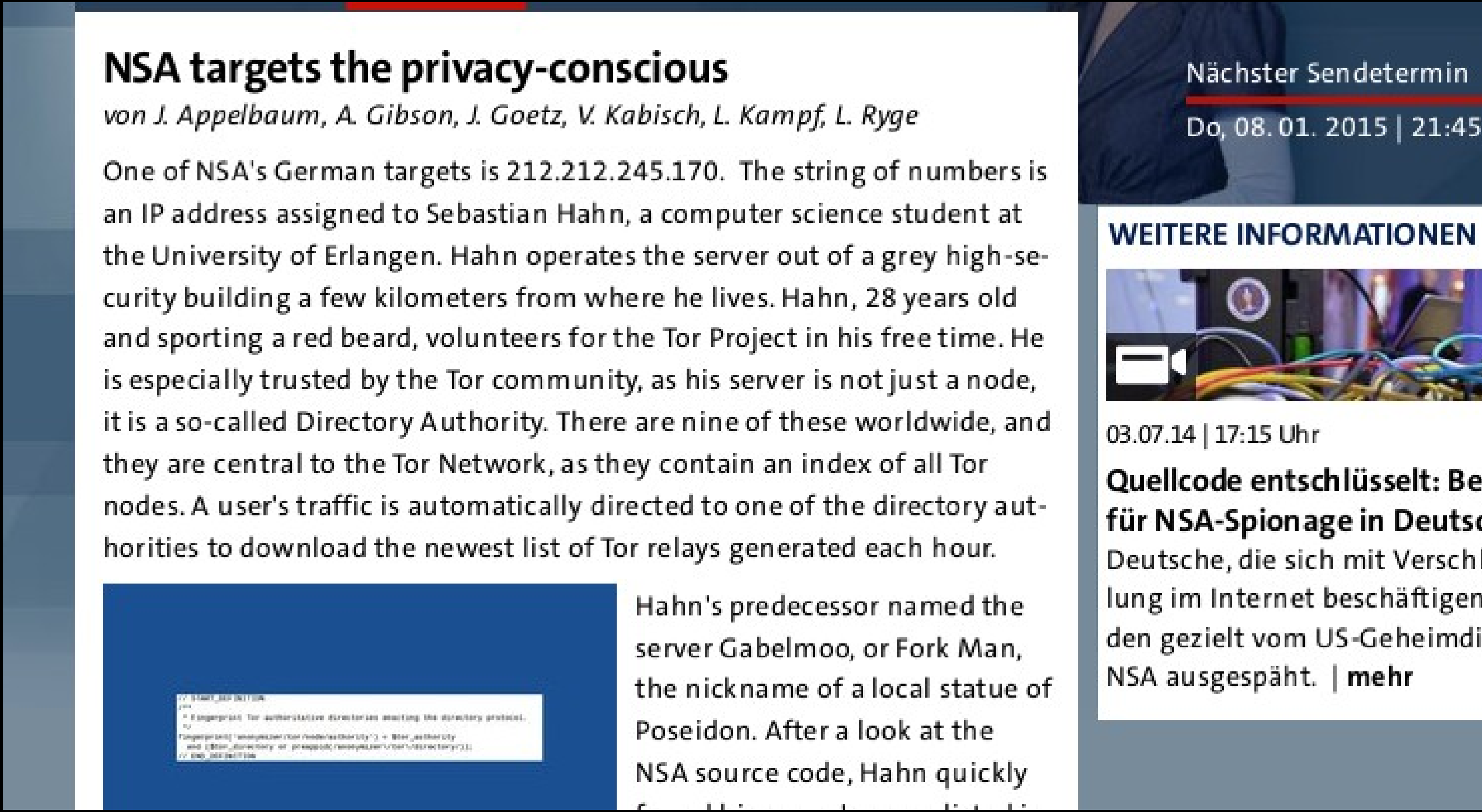


Tor
I Support Online Rights
ELECTRONIC FRONTIER FOUNDATION EFF.ORG

"Still the King of high secure, low latency Internet Anonymity"

Contenders for the throne:

- None



NSA targets the privacy-conscious

von J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge

One of NSA's German targets is 212.212.245.170. The string of numbers is an IP address assigned to Sebastian Hahn, a computer science student at the University of Erlangen. Hahn operates the server out of a grey high-security building a few kilometers from where he lives. Hahn, 28 years old and sporting a red beard, volunteers for the Tor Project in his free time. He is especially trusted by the Tor community, as his server is not just a node, it is a so-called Directory Authority. There are nine of these worldwide, and they are central to the Tor Network, as they contain an index of all Tor nodes. A user's traffic is automatically directed to one of the directory authorities to download the newest list of Tor relays generated each hour.

```
// START_DEFINITION
/**
 * Fingerprint Tor authoritative directories enacting the directory protocol.
 */
fingerprint('anonymizer/tor/node/authority') = $tor_authority
  and ($tor_directory or preappid(/anonymizer\/tor\/directory/));
// END_DEFINITION
```

Hahn's predecessor named the server Gabelmoo, or Fork Man, the nickname of a local statue of Poseidon. After a look at the NSA source code, Hahn quickly

Nächster Sendetermin

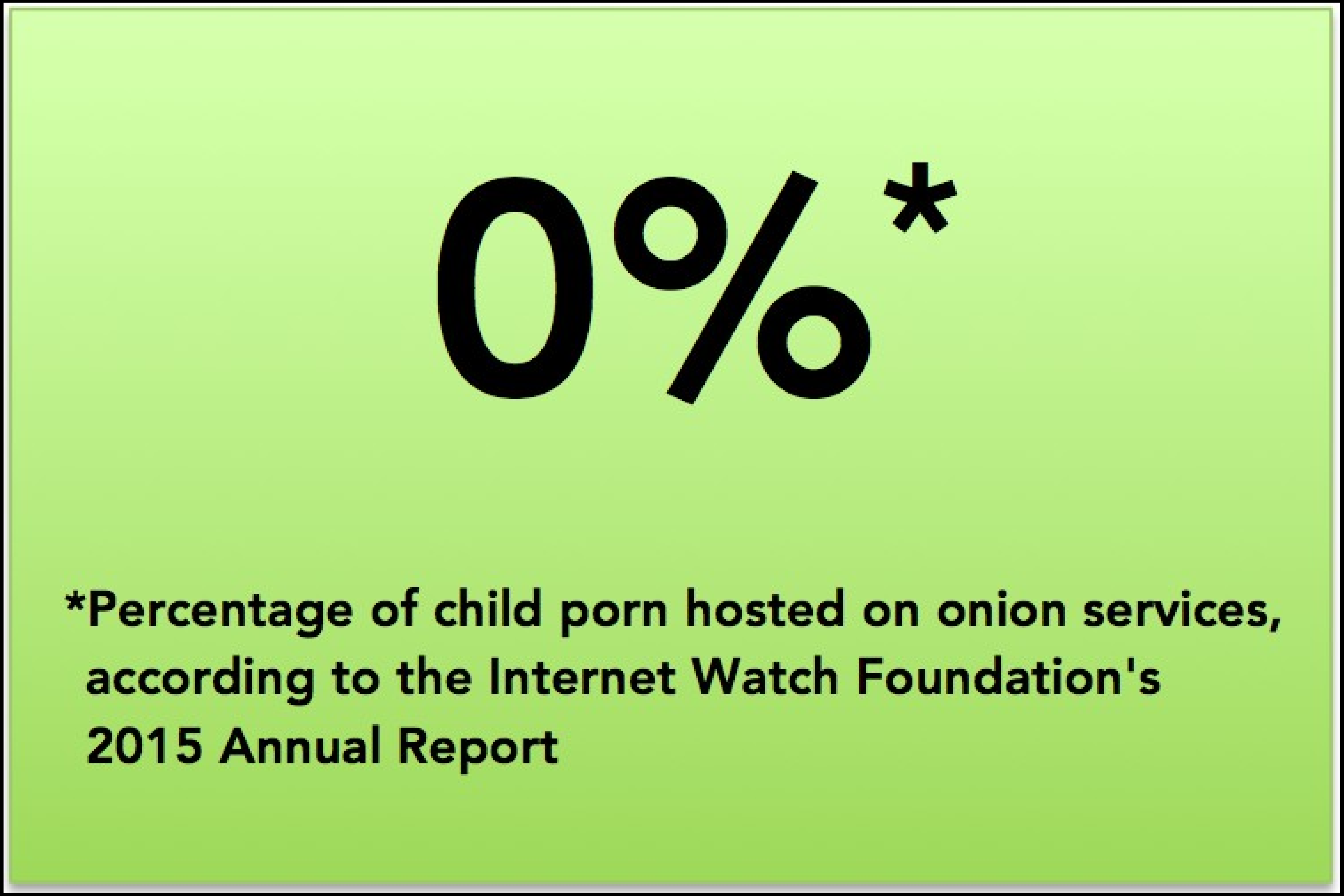
Do, 08. 01. 2015 | 21:45

WEITERE INFORMATIONEN

03.07.14 | 17:15 Uhr

Quellcode entschlüsselt: Be
für NSA-Spionage in Deutsc

Deutsche, die sich mit Verschl
lung im Internet beschäftigen
den gezielt vom US-Geheimdi
NSA ausgespäht. | **mehr**



0%*

*Percentage of child porn hosted on onion services, according to the Internet Watch Foundation's 2015 Annual Report