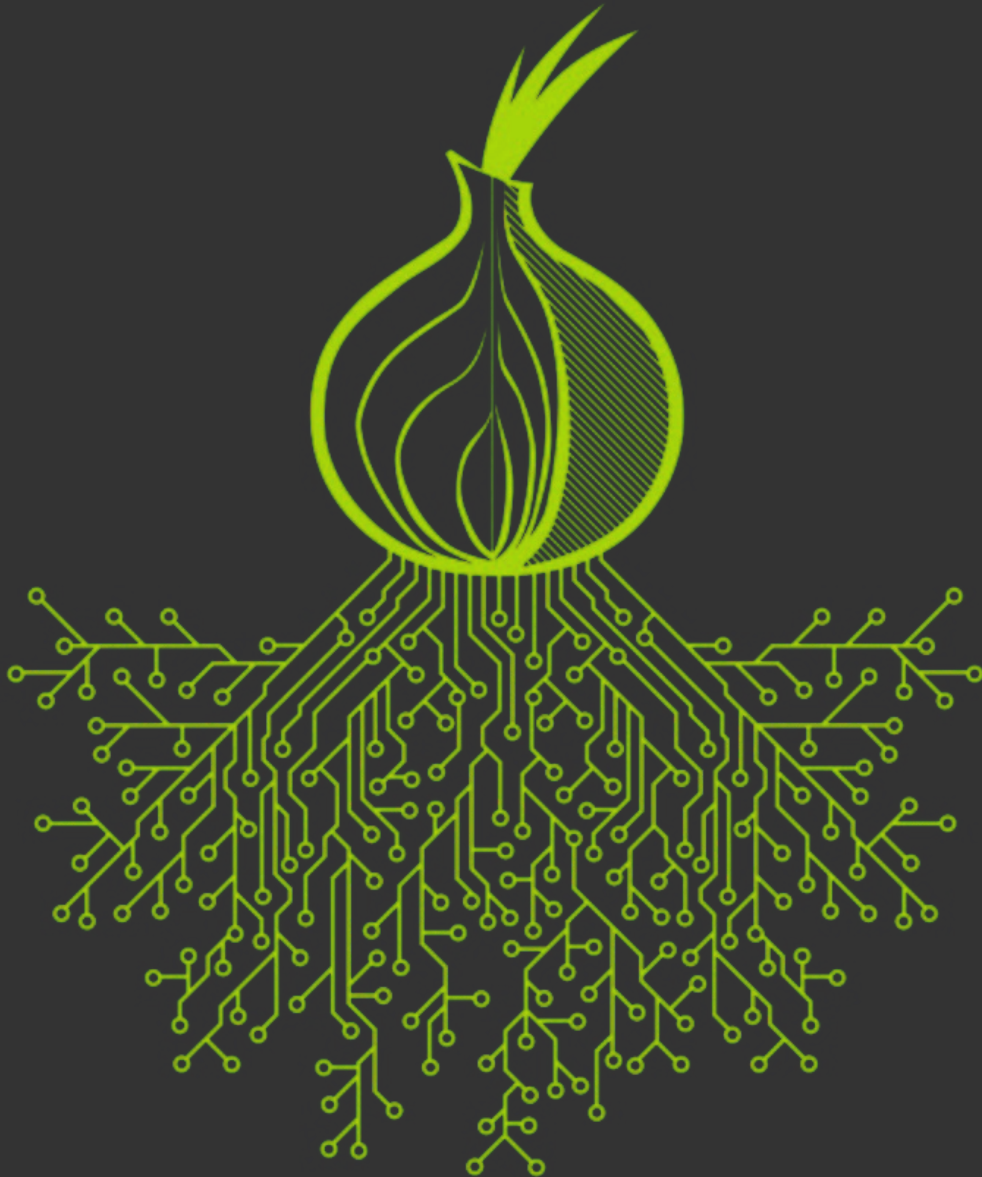


The Tor Project



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.

Tor Onion Services

More useful than you think



JOSEPH COX SECURITY 06.18.15 7:00 AM

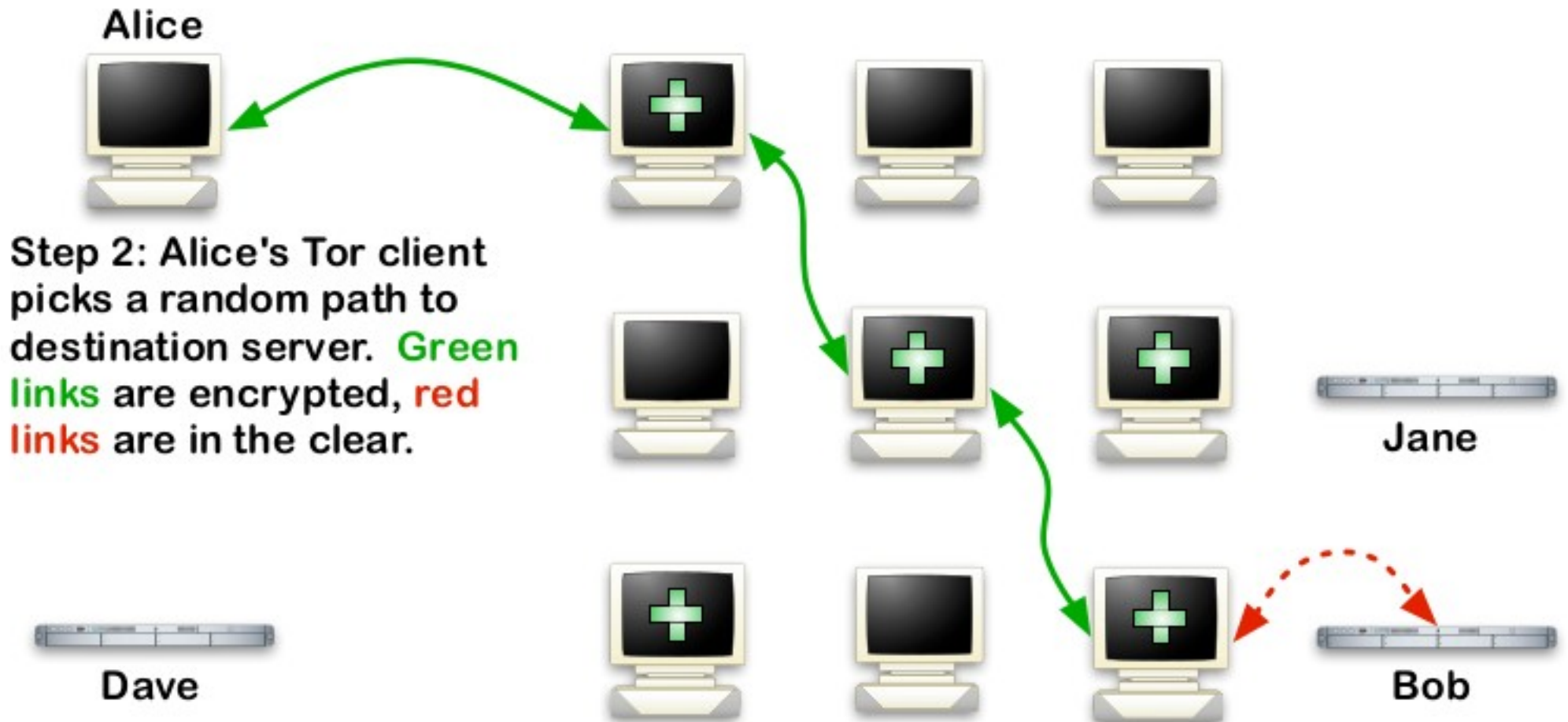
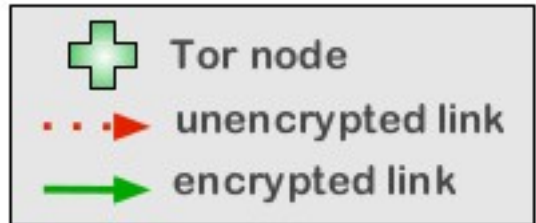
**THE DARK WEB AS YOU KNOW
IT IS A MYTH**

... this talk is NOT about the
Dark Web



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

EFF How Tor Works: 2





riseup.net



Welcome to Riseup Black

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

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

[Download Bitmask](#)[Log In](#)

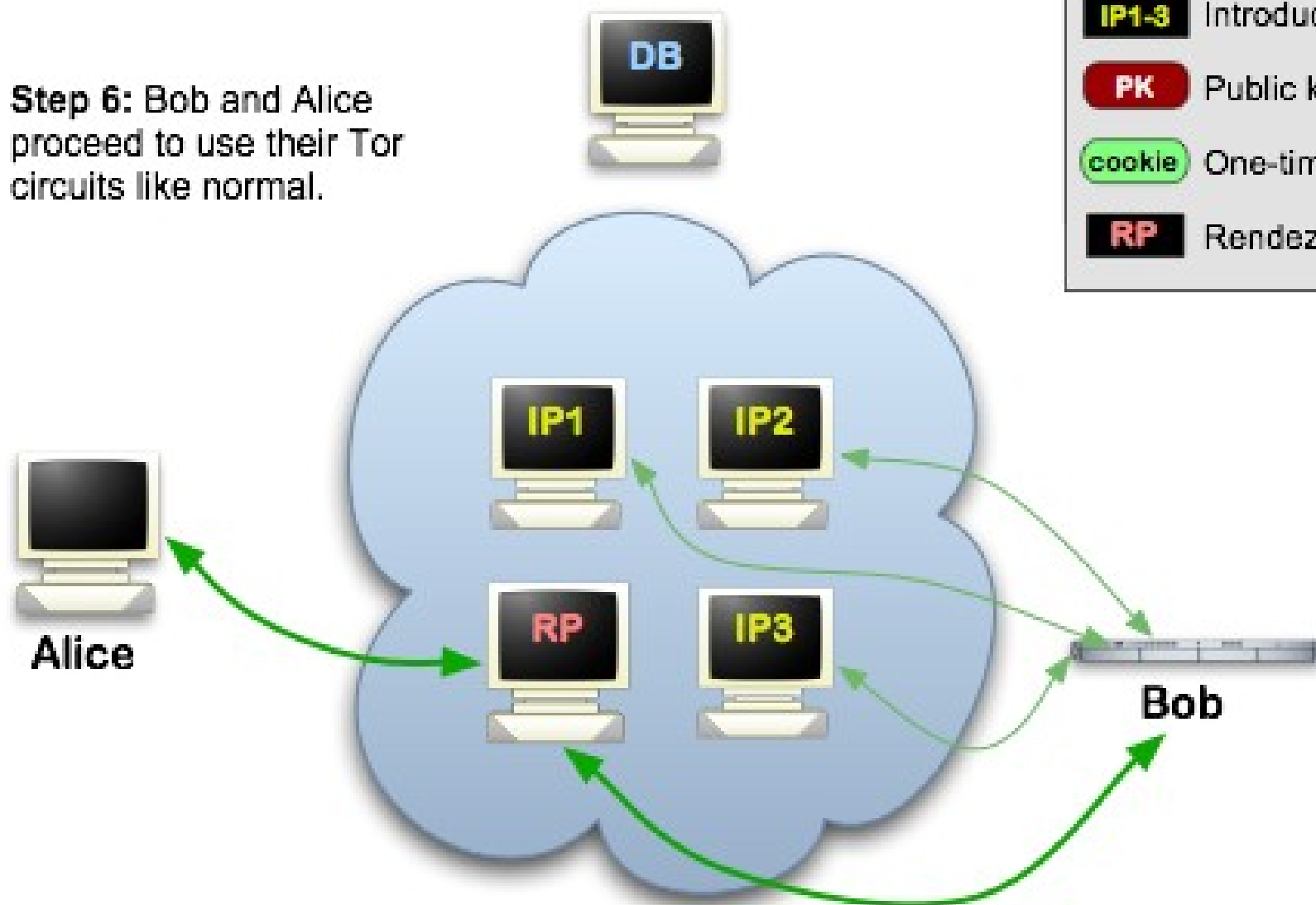
Log in to change your account settings or create support tickets for Riseup Black services.


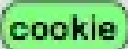

[Sign Up](#)

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.

Tor Hidden Services: 6

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



-  Tor cloud
-  Tor circuit
-  Introduction points
-  Public key
-  One-time secret
-  Rendezvous point

Onion Service Properties

Self authenticated

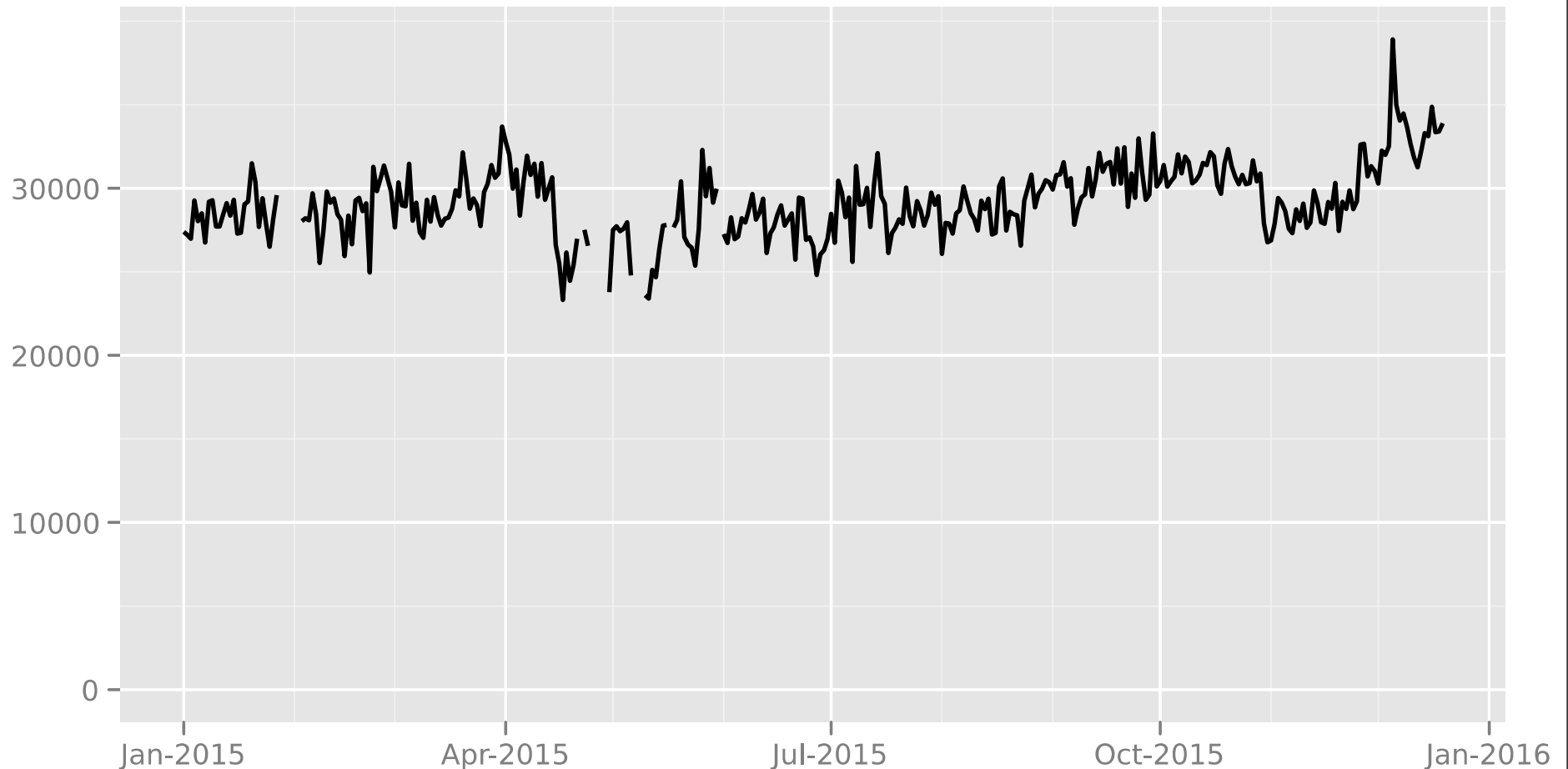
End-to-end encrypted

NAT punching

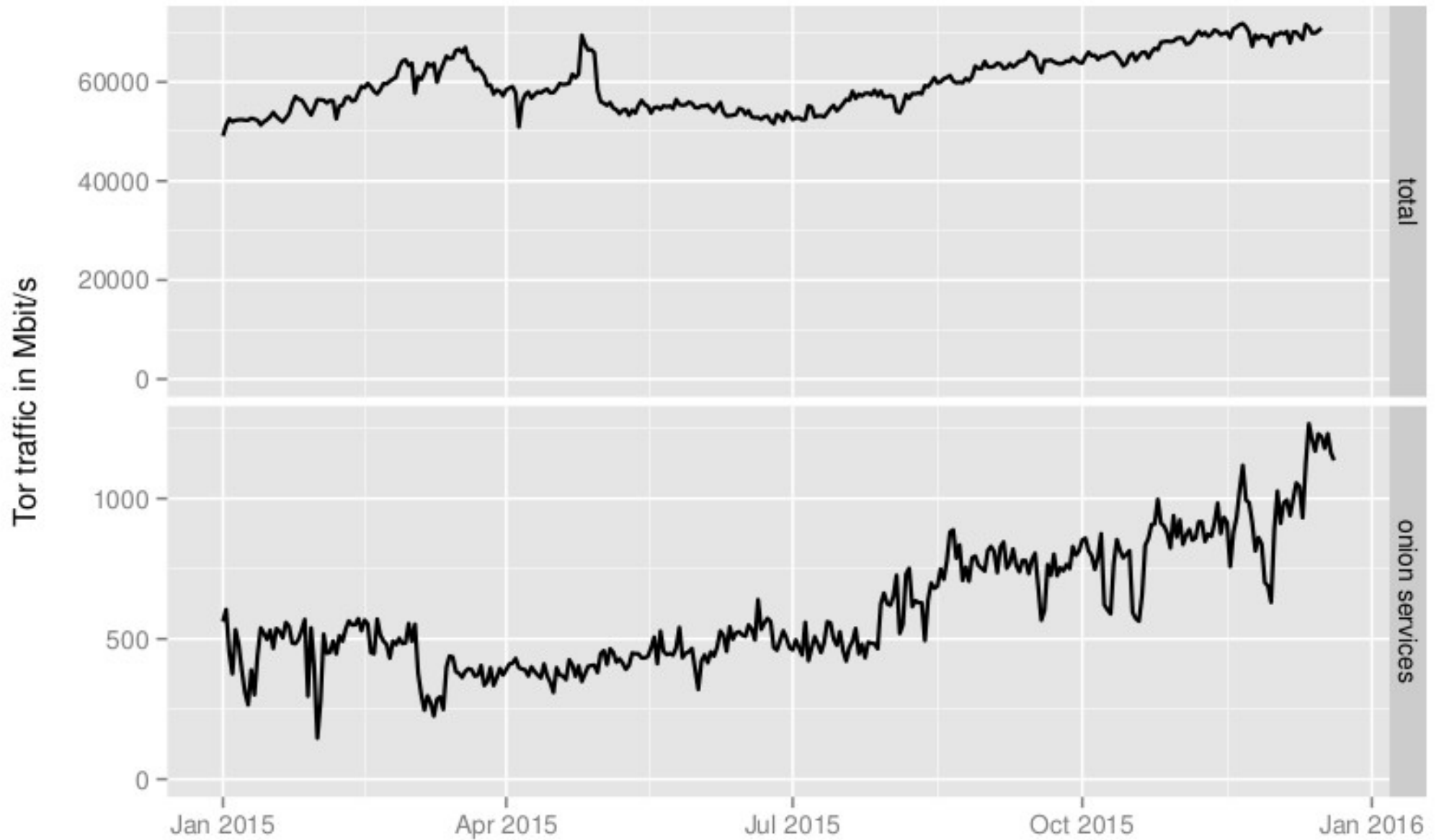
Limit surface area

Unique .onion addresses

Unique .onion addresses



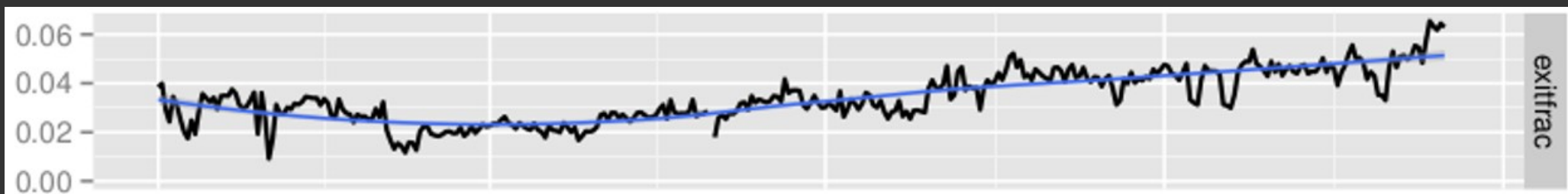
Estimated Traffic



Estimated Traffic

As of December 2015,

~5% of **client** traffic is HS



Statistics

Proposal 238

<https://research.torproject.org/tech-reports/extrapolating-hidserv-stats-2015-01-31.pdf>

Birth - 2004



ChangeLog file entry:

Changes in version 0.0.6pre1 - 2004-04-08

- o Features:

- Hidden services and rendezvous points are implemented. Go to <http://6sxoyfb3h2nvok2d.onion/> for an index of currently available hidden services. (This only works via a socks4a proxy such as Privoxy, and currently it's quite slow.)

Early use case - 2006



Wikileaks - 2007



Wikileaks:Tor

(Redirected from [Tor](#))

The following method requires some technical ability. If you are used to installing new software and configuring proxy servers you should have the required skills, otherwise you may wish to use one of our [other submission methods](#). Don't let the technology defeat you!

Tor or The Onion Router is a cryptographic technique first implemented by US navy research to permit intelligence agents to use the internet without being traced, by encrypting and routing communications through many different internet servers. Subsequently Tor has been developed by US University [MIT](#) and the California internet rights watchdog the [Electronic Frontier Foundation](#) and subsequently incorporated into [Wikileaks](#).

Using our anonymous access package ([see below](#)) you can prevent internet spies knowing that your computer has connected to [Wikileaks](#).

Most Wikileakers will not need this extra security and there are simpler and possibly safer alternatives for once-off high-risk leaks (see [Submissions](#)). But for those who are at risk and want to access Wikileaks from the comfort of their homes or offices or need to bypass [Internet Censorship](#), Tor ([Onion Routing](#)) is an excellent solution.

When you have installed our Tor access package (see below), you may then connect to [Wikileaks](#) via our anonymous address (the ".onion" is short for "Onion Routing", but you do not need to be concerned with this detail).

Then whenever you want to establish an encrypted anonymous (even to internet spies) connection to [Wikileaks](#) goto our magic link:

<http://gaddbiwdfapglkq.onion/>

(this link will only work once you have installed and configured Tor)

To upload a document anonymously using tor:

<http://gaddbiwdfapglkq.onion/wiki/Special:Leak>

(this link will only work once you have installed and configured Tor)

Unless your memory is superb you may wish to write that address down, but make sure you discard the paper after you are finished with it.

Without Tor, when you access a Wikileaks site the usual way, e.g via <https://wikileaks.org/> all your data is encrypted, but internet spies maybe able note how long your computer spent talking to Wikileaks servers. See [Connection Anonymity](#) for further discussion.

GlobalLeaks - 2011



Today, more than 30 projects use GlobalLeaks

<https://en.wikipedia.org/wiki/GlobalLeaks#Implementations>

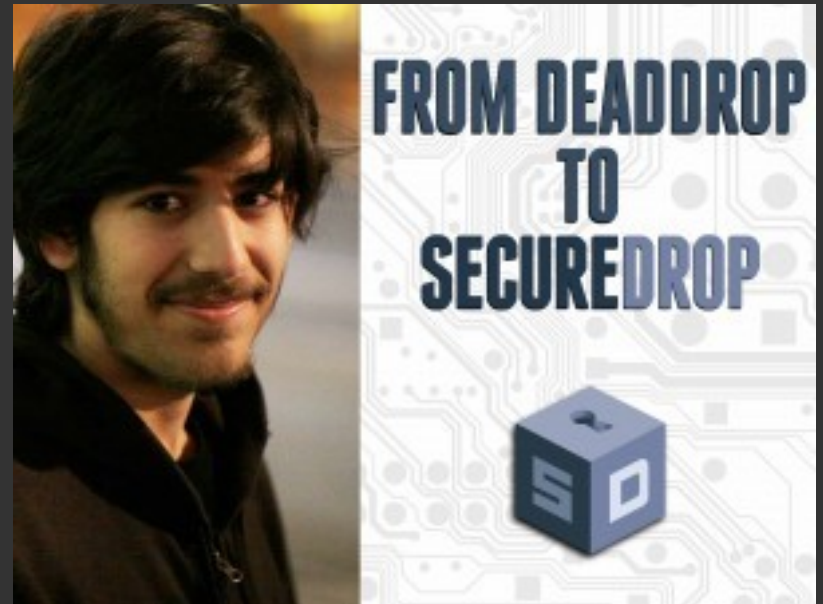


GlobalLeaks - WildLeaks



WildLeaks
WILDLIFE

SecureDrop - 2013



Today, 22 organizations use SecureDrop

<https://securedrop.org/directory>

Aphex Twin release - 2014



Aphex Twin ✓

@AphexTwin



Follow

<http://syro2eznzea2xbpi.onion>

RETWEETS

3,801

LIKES

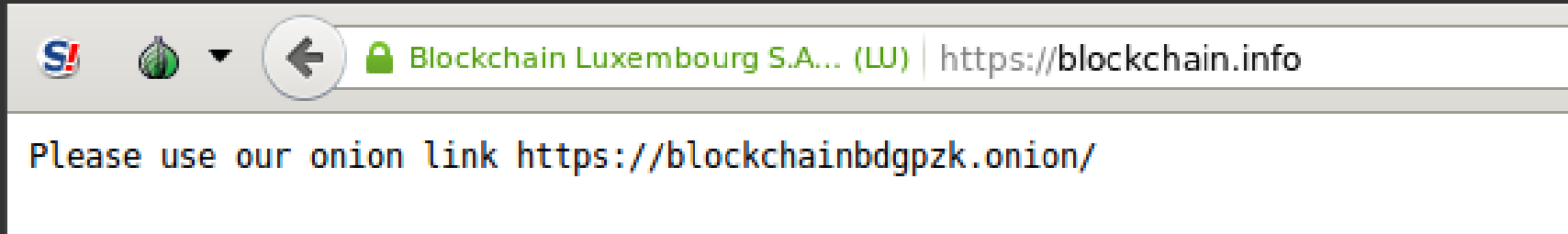
2,943



8:00 AM - 18 Aug 2014



Blockchain - 2014



Security concerns.

Avoid exit node attack rewriting bitcoin addresses.

And Facebook Too - 2015

- No more worrying about **bad** certificate authorities
- Avoids exit relay contention, traffic **never leaves** the network!
- Ultimately it could be **faster** than reaching Facebook with a normal Tor circuit

Public Website

Onion addresses for public websites makes **perfect sense**:

it gives users the choice of what security properties they **want**

.onion and EV cert



- Browsers know to treat cookies/etc like **TLS**
- Server-side does **not** need to treat .onion specially
- With an EV cert, the browser shows the user that it's **really** Facebook

Magic of .onion EV certs!

Onion SSL Certificates have a
magic extra feature,

The only EV SSL Certs which can
use wildcards!

Let's Encrypt - 2015

- What might this look like at scale?
- Bundle Tor with Let's Encrypt, so every website can add an onion address in its certificate?
- (Some technical and policy barriers remain)



RFC7686 - 2015

Internet Engineering Task Force (IETF)
Request for Comments: 7686
Category: Standards Track
ISSN: 2070-1721

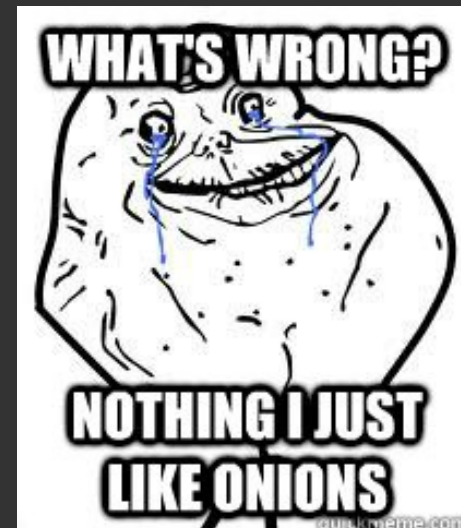
J. Appelbaum
The Tor Project, Inc.
A. Muffett
Facebook
October 2015

The ".onion" Special-Use Domain Name

Abstract

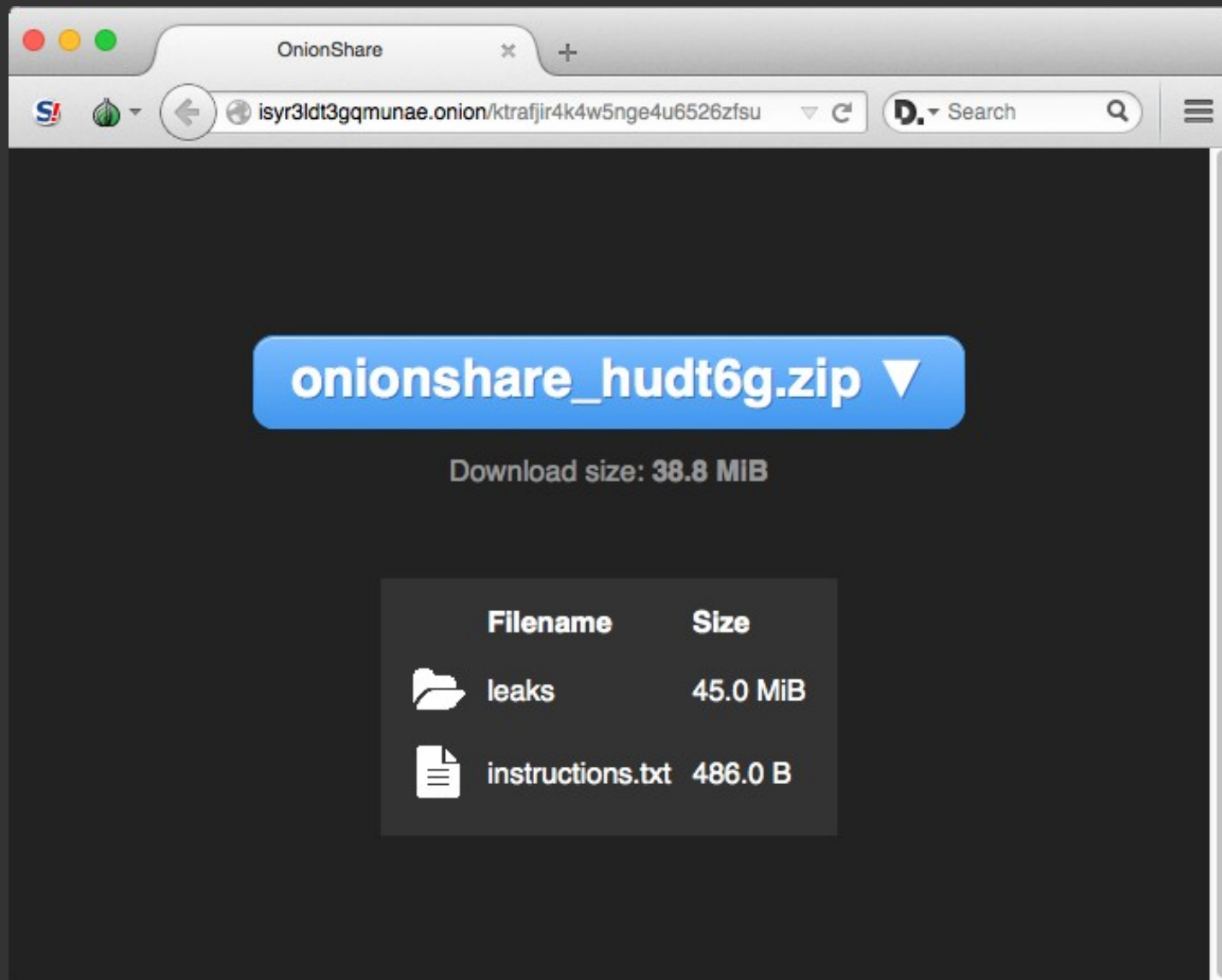
This document registers the ".onion" Special-Use Domain Name.

We haz the .onion!



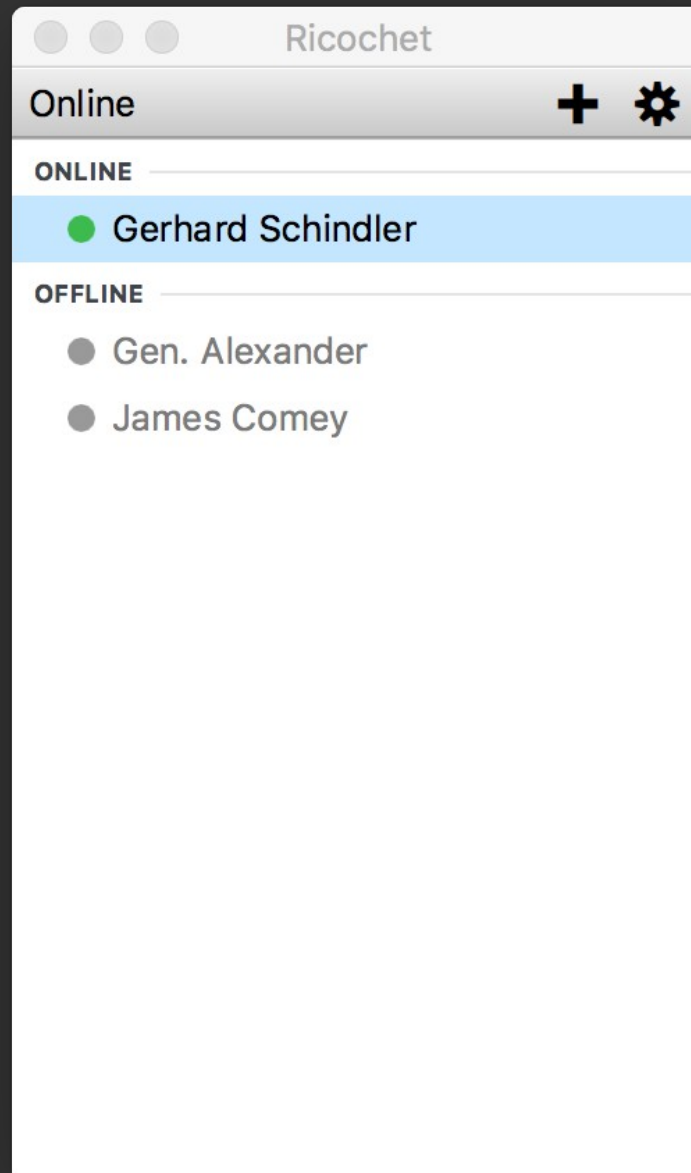
OnionShare

<https://onionshare.org/>



Ricochet

<https://ricochet.im>



Pond

<https://pond.imperialviolet.org>

Pond

Create Account

In order to use Pond you have to have an account on a server. Servers may set their own account policies, but the default server allows anyone to create an account. If you want to use the default server, just click 'Create'.

Server:

Create

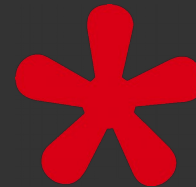
Services and Tools



All Riseup.net services are available using hidden service

<https://help.riseup.net/en/tor#riseups-tor-hidden-services>

... and many others



...



debian

Package repository

<http://vwakviie2ienjx6t.onion/>

```
apt-get install apt-tor-transport
```

Many Other Services



We know of several Alexa top 500 sites that are currently deploying hidden services



Help us have more!

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.**

Excitement in Pittsburgh



Did the FBI Pay a University to Attack Tor Users?

Posted November 11th, 2015 by arma in [CMU](#), [ethics](#), [hidden services](#), [onion services](#)

The million-dollar hole in the FBI 'paying CMU to crack Tor' story

Did Carnegie Mellon Attack Tor for the FBI?

There's [pretty strong evidence](#) that the team of researchers from Carnegie Mellon University who cancelled their [scheduled 2015 Black Hat talk](#) deanonymized Tor users for the FBI.

Ethics

...Should we start a Tor ethics review board?

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?

Tor Hidden Services: 1

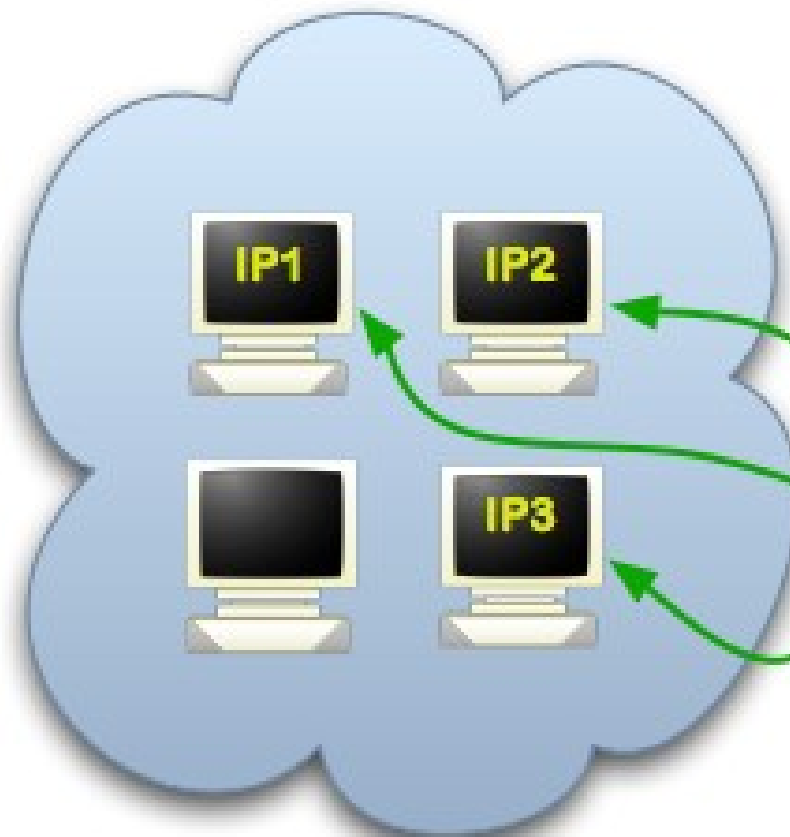
Step 1: Bob picks some introduction points and builds circuits to them.



Alice



DB



Tor cloud



Tor circuit

IP1-3

Introduction points

PK

Public key

cookie

One-time secret

RP

Rendezvous point



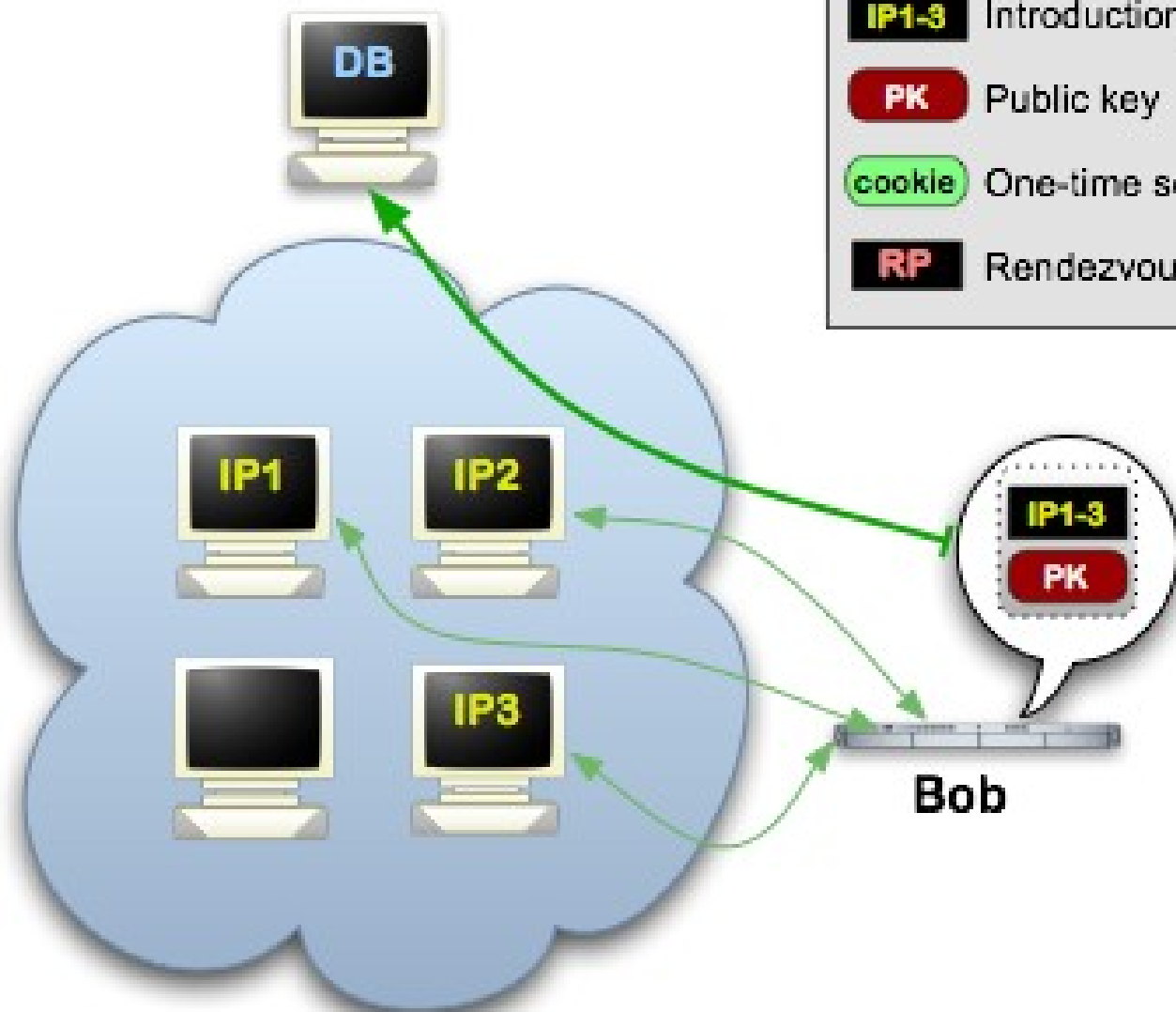
Bob

Tor Hidden Services: 2

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

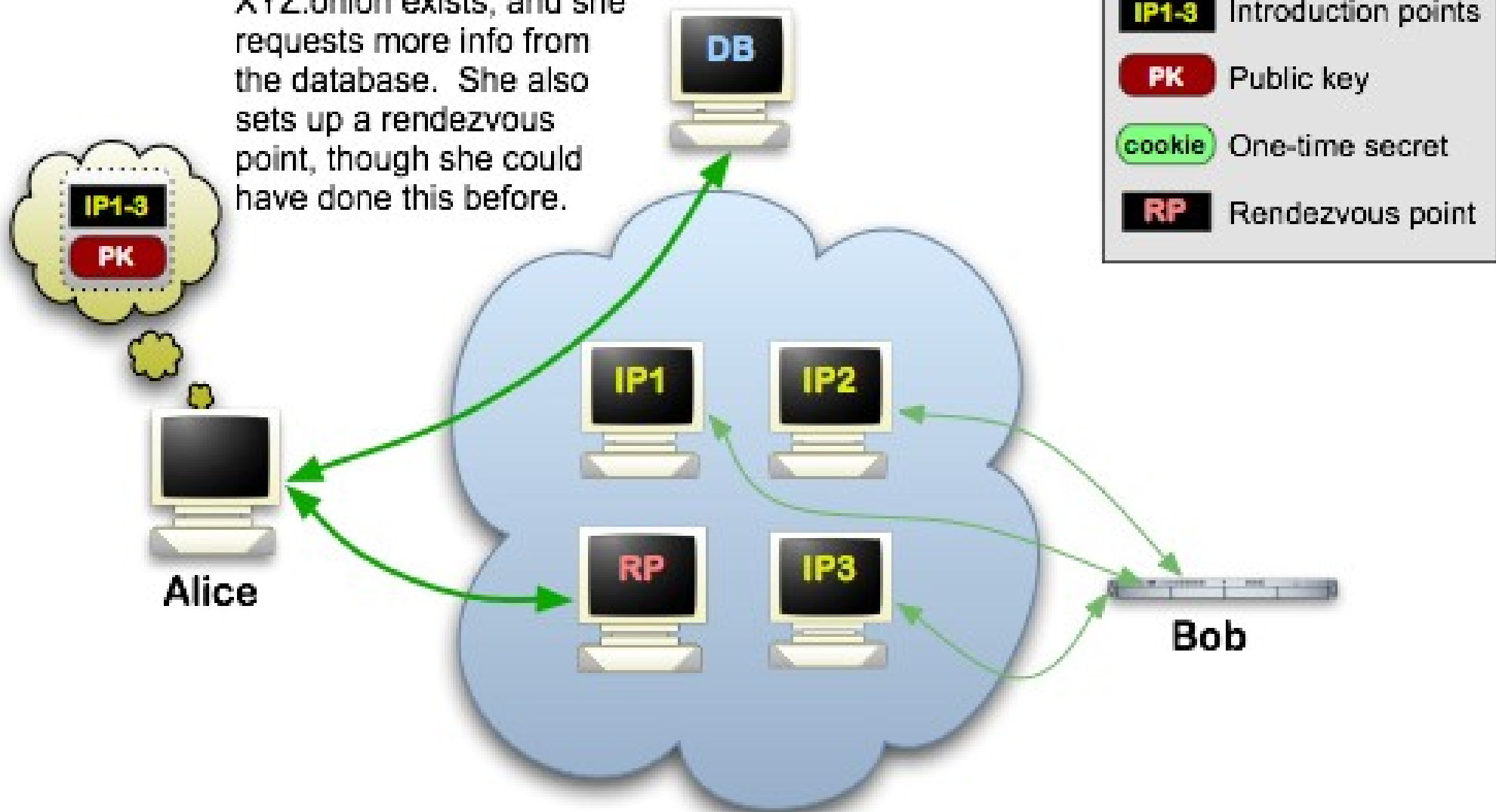


Alice



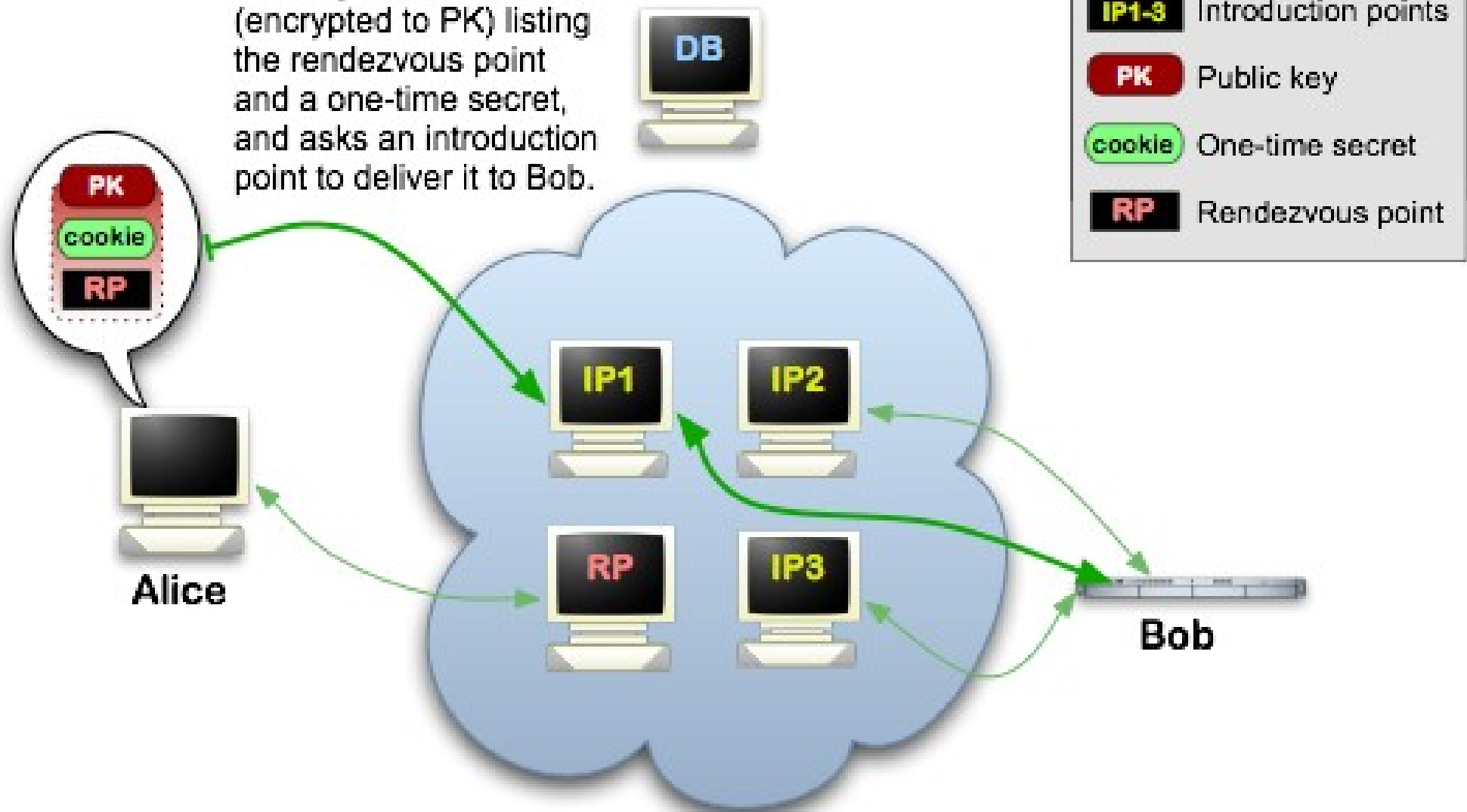
Tor Hidden Services: 3

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.



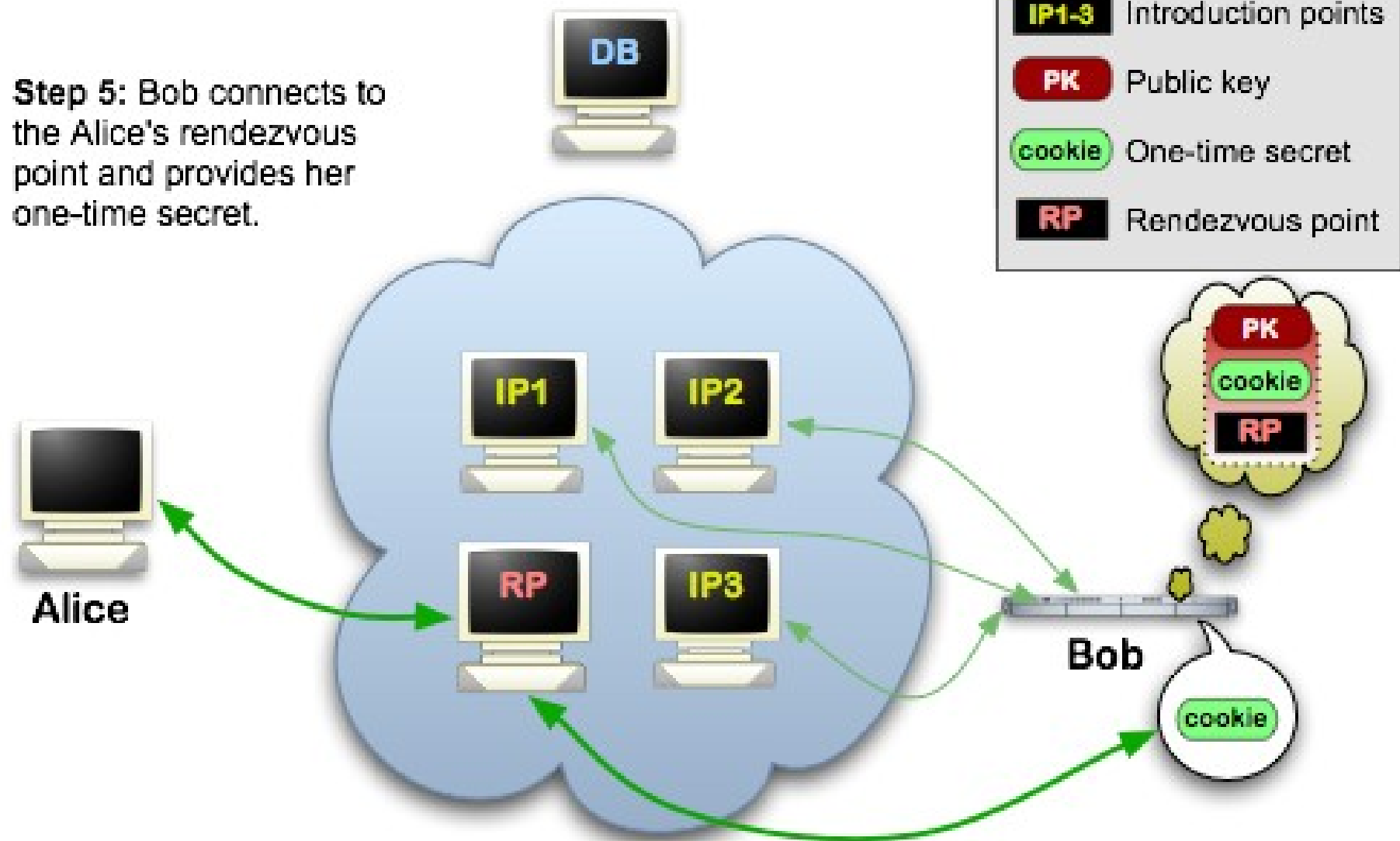
Tor Hidden Services: 4

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.



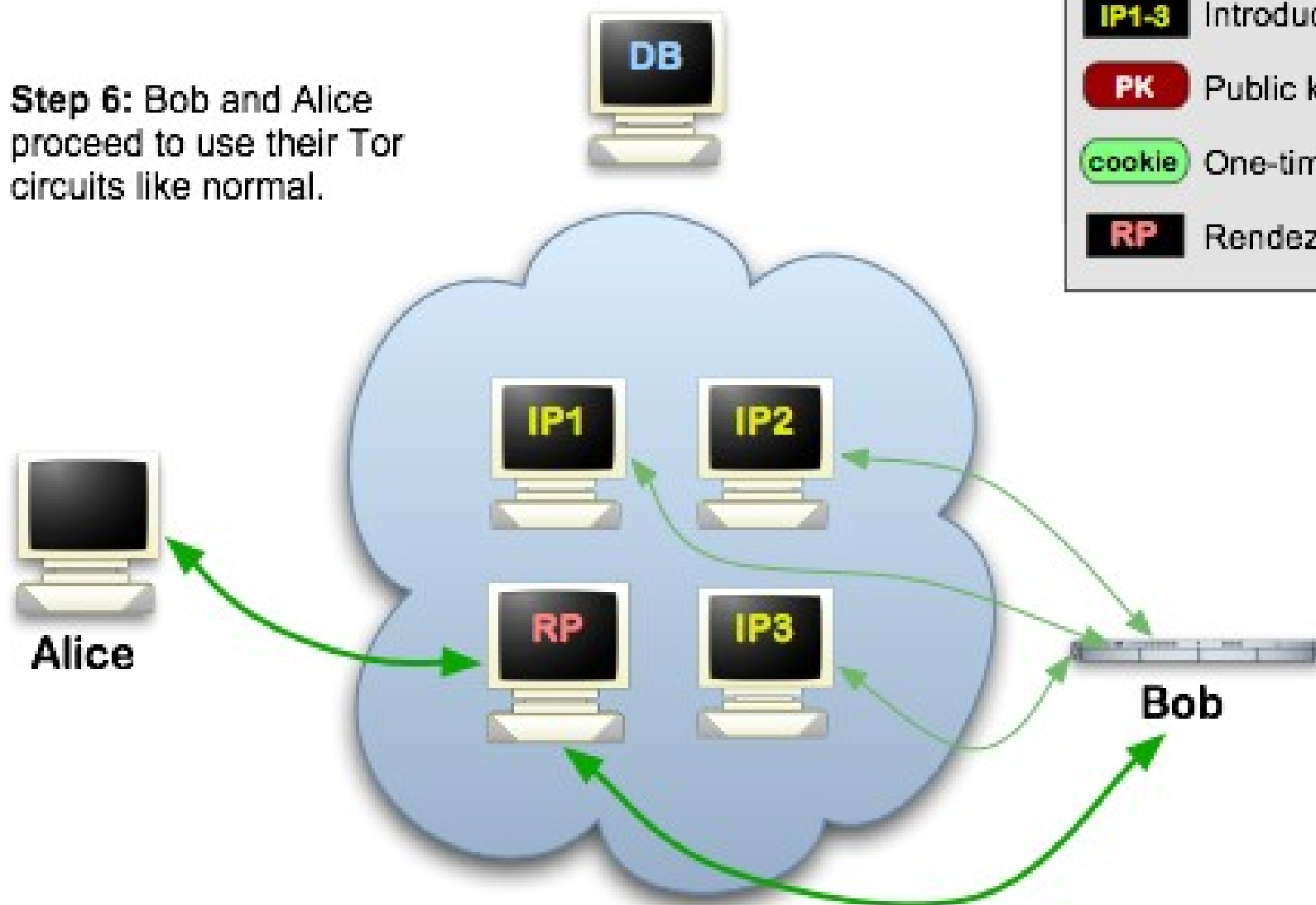
Tor Hidden Services: 5

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



Tor Hidden Services: 6

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



HS Directory

Desc ID = $H(\text{onion-address} \mid H(\text{time-period} \mid \text{descriptor-cookie} \mid \text{replica}))$



Next Generation Onion Service (NGOS)

Proposal 224

blob: 8dd30b0e95d4ff5695eebd7a73f894ce825bc587 ([plain](#))

1	Filename: 224-rend-spec-ng.txt
2	Title: Next-Generation Hidden Services in Tor
3	Author: Nick Mathewson
4	Created: 2013-11-29
5	Status: Draft

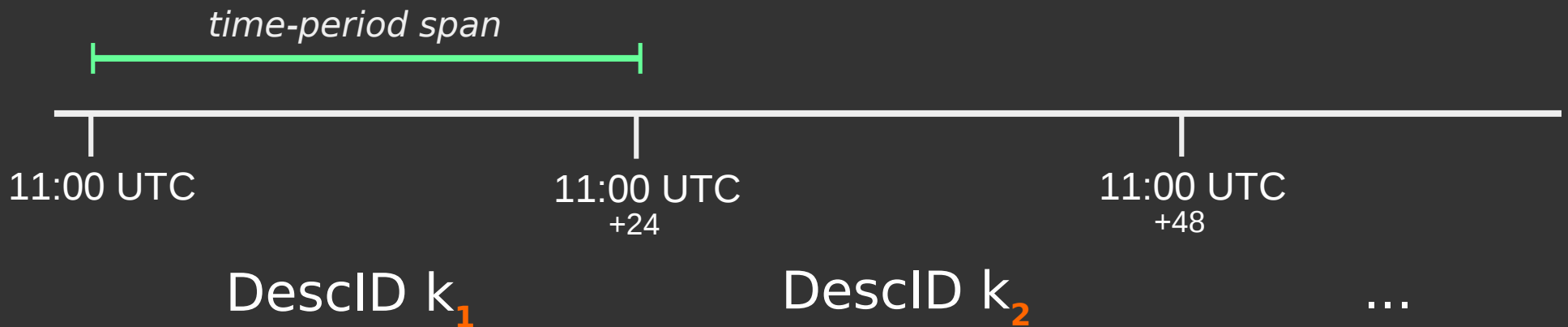


Created: 2013-11-29

HSDir Predictability

Desc ID = $H(\text{onion-address} \mid H(\text{time-period} \mid \text{descriptor-cookie} \mid \text{replica}))$

 Invariant

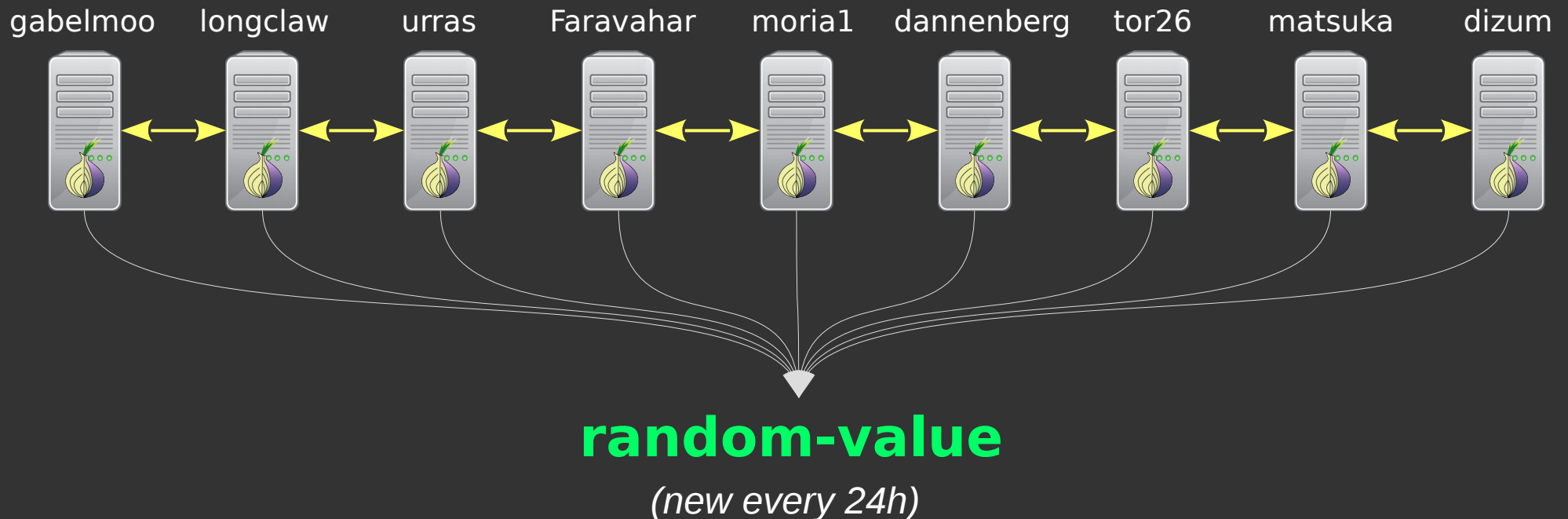


Shared Randomness

Proposal 250

Desc ID = $H(\text{onion-address} \mid H(\text{time-period} \mid \text{random-value} \mid \text{descriptor-cookie} \mid \text{replica}))$

 Invariant



Better Crypto



Bigger Onion Address

From 16 characters:

nzh3fv6jc6jskki3.onion

... to 52 characters:

a1uik0w1gmfq3i5ievxdm9ceu27e88g6o7pe0rffdw9jmntwkdsd.onion

(ed25519 public key base32 encoded)

Rendezvous Single Onion Services (RSOS)

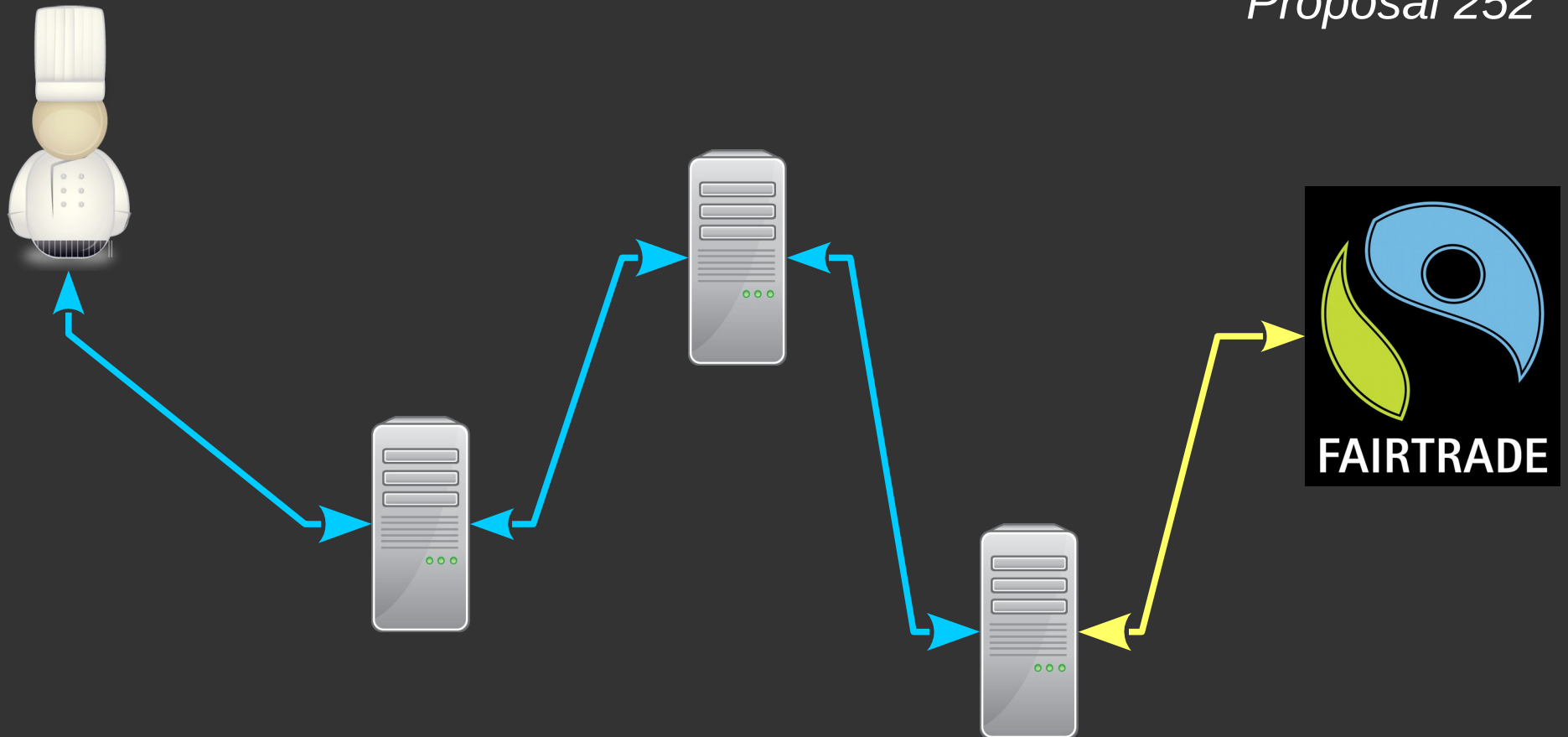
Proposal 260



Rendezvous Point

Single Onion Services (SOS)

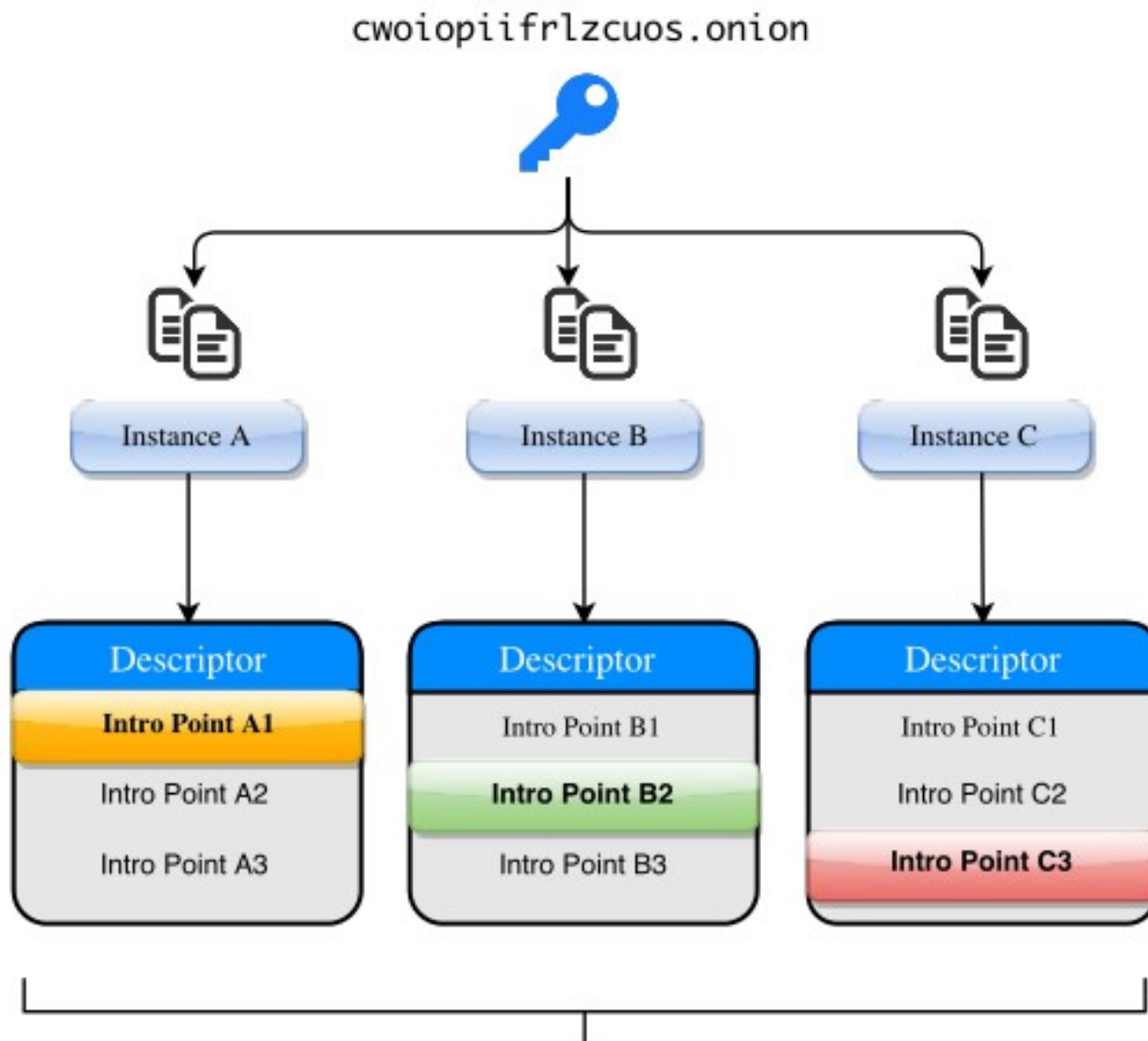
Proposal 252



The circuit is extended to the service.
No Introduction nor Rendezvous.

OnionBalance - TSoP

<https://onionbalance.readthedocs.org>



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

THIS IS WHAT A
Tor



SHARI STEELE AND HER DAUGHTER HANNA

SUPPORTER
LOOKS LIKE

#SUPPORT**Tor**

revolution and
dissent.

Molly Crabapple

ARTIST, WRITER, ENTREPRENEUR

een
e
other

ts.
Tor to
ces
reely.
ool,

S



#SUPPORT**Tor**



#SUPPORT**Tor**

Question Time!

THIS IS WHAT A
Tor



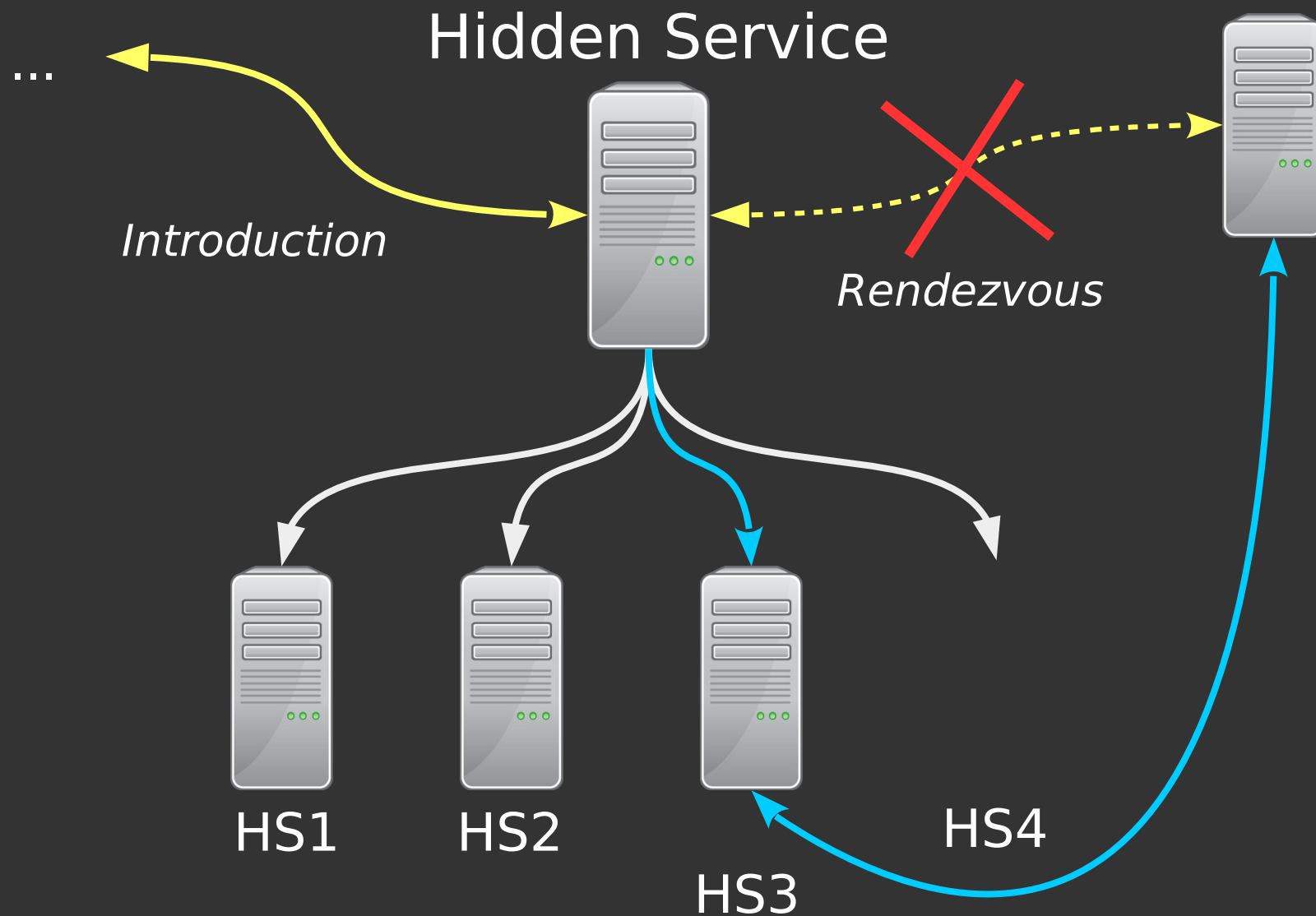
DOCTOROW FAMILY

SUPPORTER
LOOKS LIKE

#SUPPORT**Tor**

Load Balancing

Proposal 255



Easy Deployment

Apaf

ADD_ONION