Lecture 9: Onion Routing and Tor

CPSC 444/544 Real-World Cryptography
2026 Spring

Prof. Fan Zhang

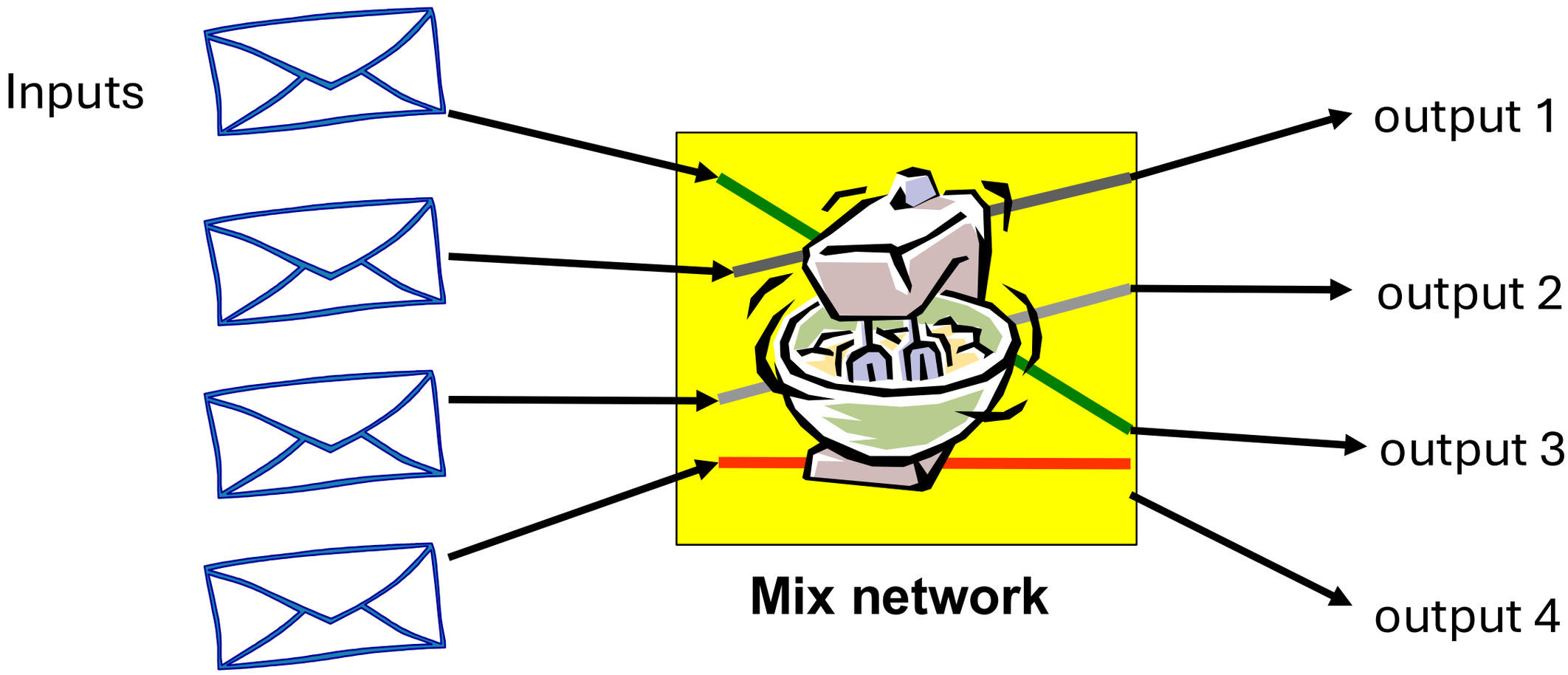
Yale

Computer Science

Recap

- "If we know enough metadata, we don’t really need the content”
- **Anonymity** is about hiding metadata that links actions to identities
- **Anonymity set: a crowd to blend in**
  - A way to quantify anonymity
- Next up: Tor, which is low-latency, but does not withstand a global network adversary.

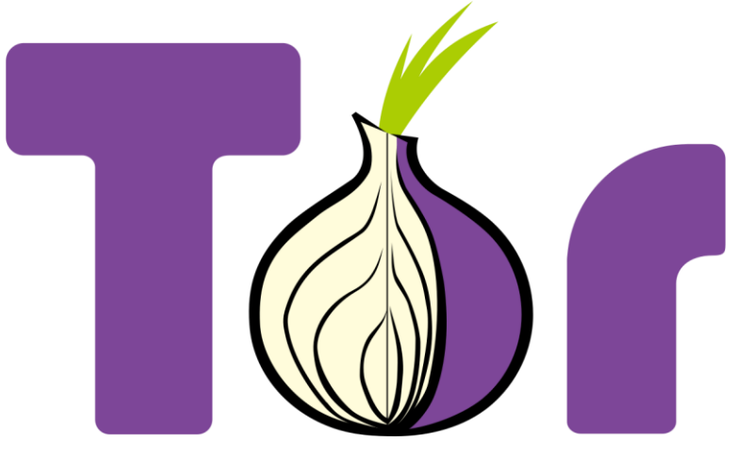
Mixnet



Batch, decrypt/re-encrypt, permute, forward

Tension: High anonymity ⇒ high latency

Tor: the onion router



Tor: The Second-Generation Onion Router

Roger Dingledine
The Free Haven Project
arma@freehaven.net

Nick Mathewson
The Free Haven Project
nickm@freehaven.net

Paul Syverson
Naval Research Lab
syverson@itd.nrl.navy.mil

USENIX Security ‘04

Why Tor?

- Mixnet not usable for latency-sensitive applications (e.g., Web)
- To reduce latency:
  - Don’t batch -- forward packets right away
- How about traffic analysis?
  - Made hard by choosing random routes
  - Nonetheless possible by powerful adversary.
- Most importantly, it is actually *usable*.

Download Tor Browser

Protect yourself against tracking, surveillance, and censorship.

Download for Windows

Signature

Download for macOS

Signature

Download for Linux

Signature

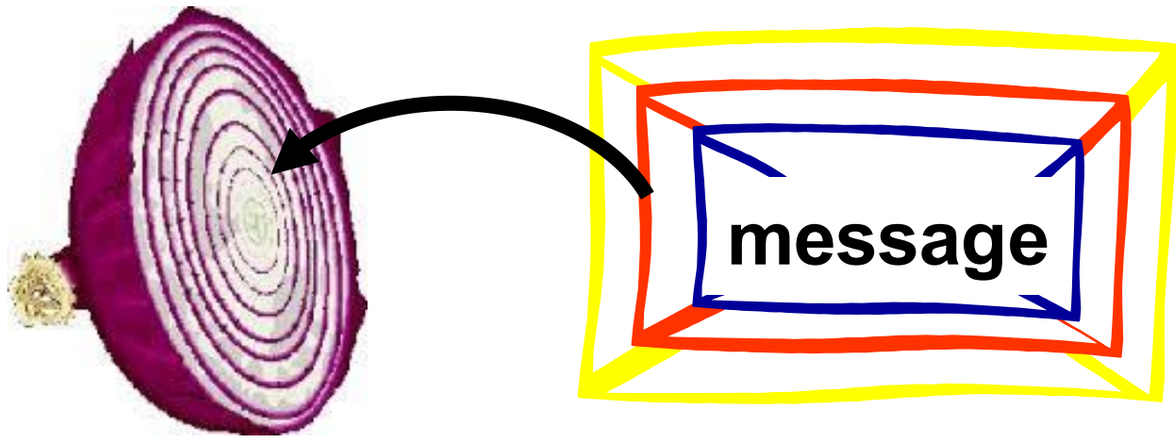
Download for Android

Download for another platform

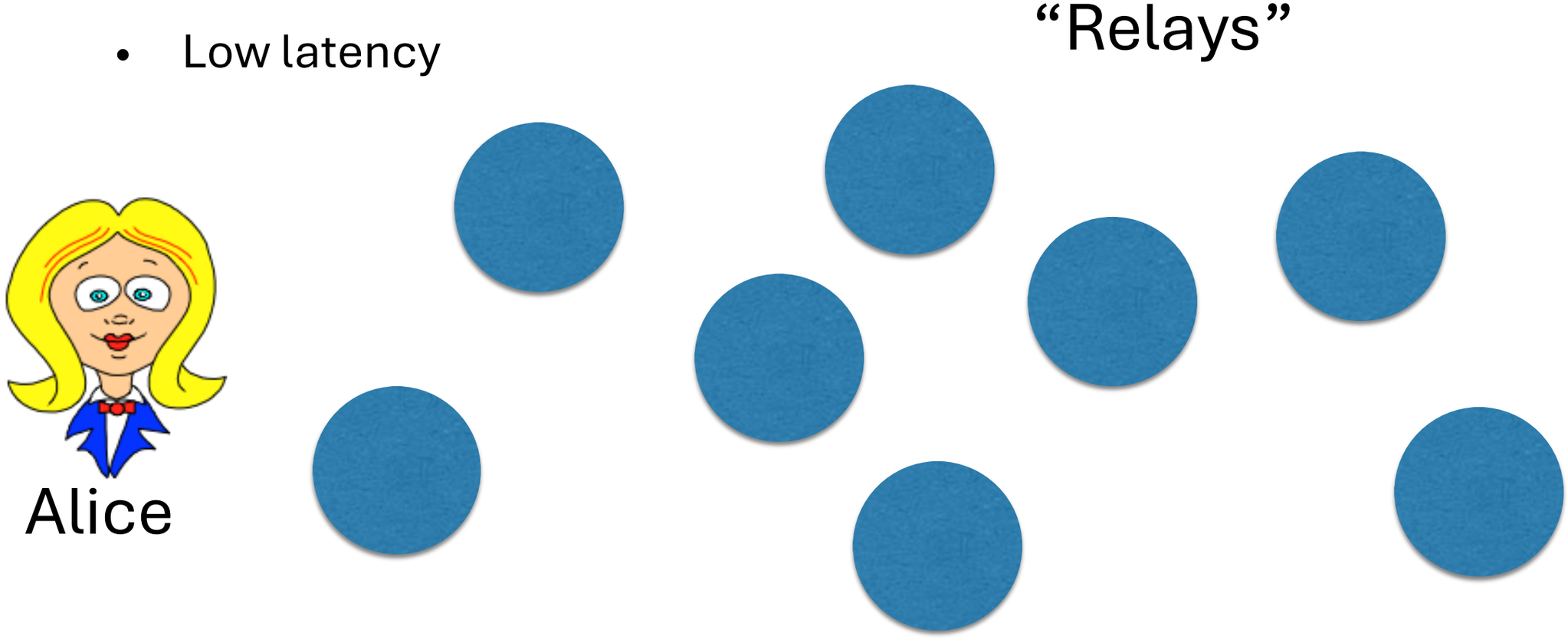
Download the latest alpha build

Download Tor

Onion routing

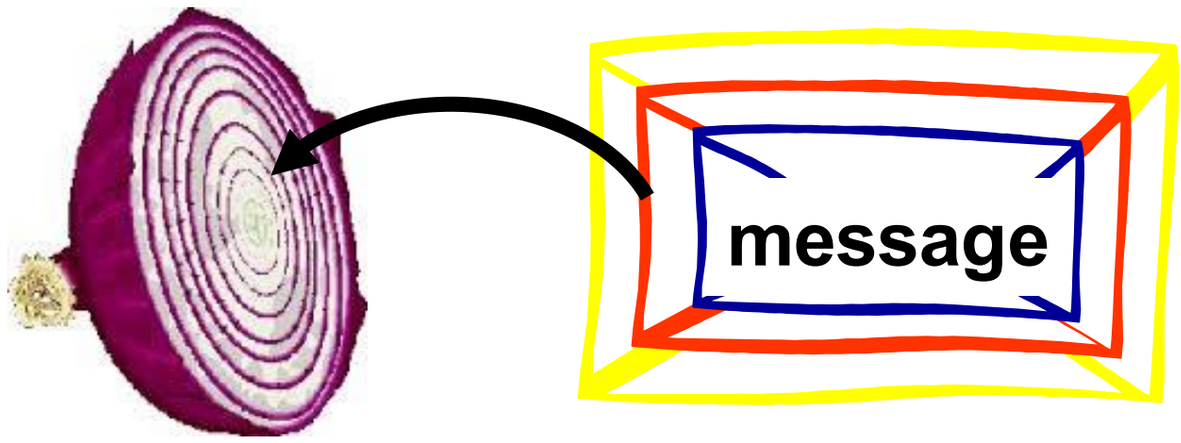


- Tor is an implementation of **Onion routing** with optimizations
- Asynchronous construction:
  - No batching!
  - Low latency

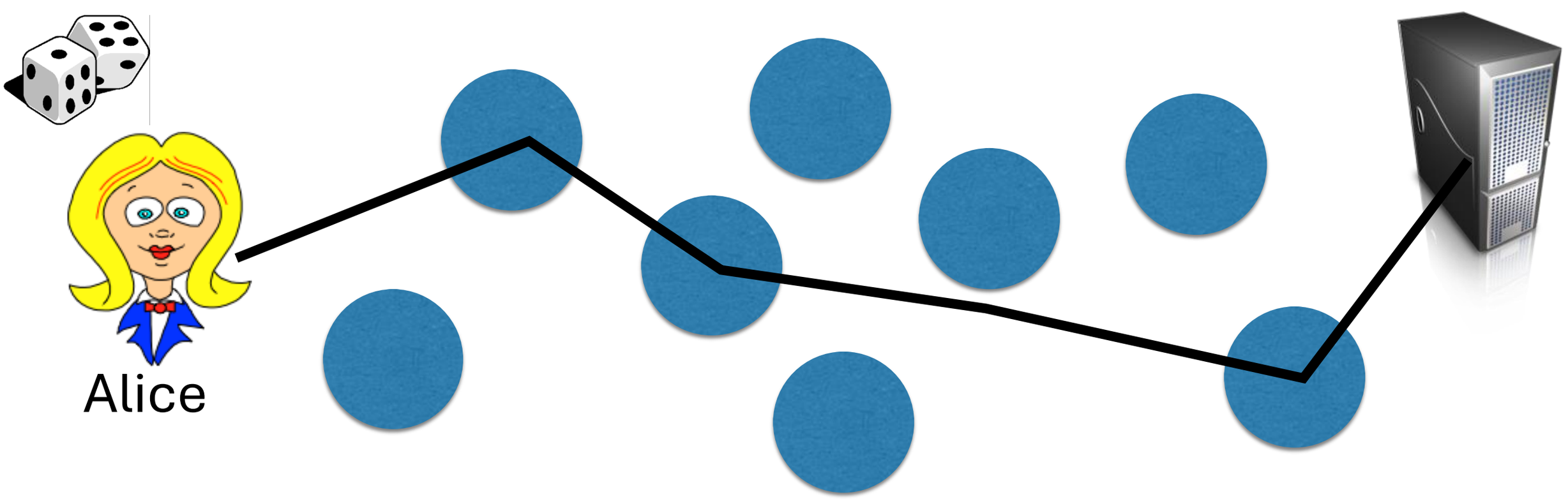


[M.G. Reed, P.F. Syverson, and D.M. Goldschlag. Anonymous connections and onion routing. IEEE SAC 16 (4), 482-494, 1998.]

Onion routing

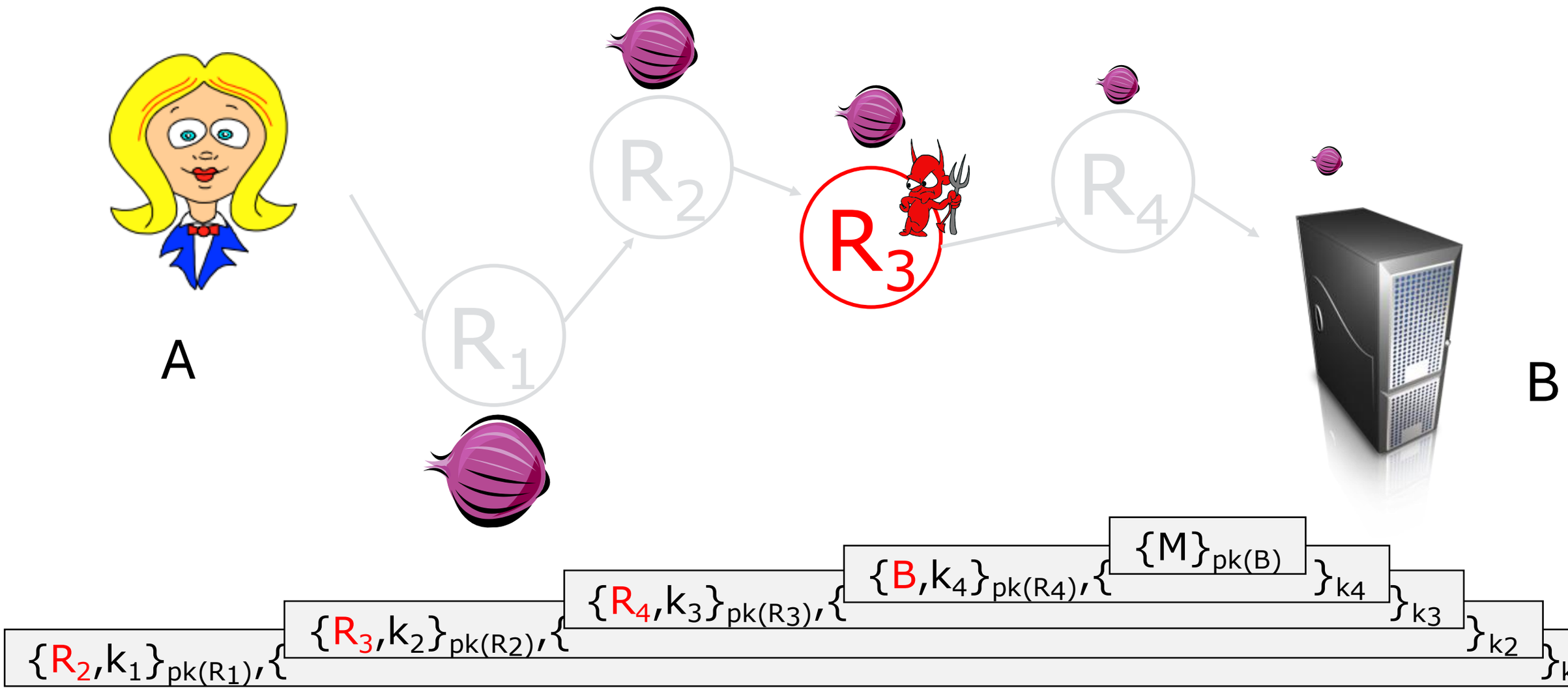


1. User (Alice) obtains relay info from a directory.
2. User *randomly selects a* set of relays (often three) and lays down a path.
   - Path changes from session to session.
3. Each node behaves like a mix **[Compare this to mixnet?]**



[M.G. Reed, P.F. Syverson, and D.M. Goldschlag. Anonymous connections and onion routing. IEEE SAC 16 (4), 482-494, 1998.]

Onion routing



Security property: A relay learns only the identity of the previous and next hops.

[M.G. Reed, P.F. Syverson, and D.M. Goldschlag. Anonymous connections and onion routing. IEEE SAC 16 (4), 482-494, 1998.]

R. Dingledine, N. Mathewson, P. Syverson

Tor:
The Second-Generation Onion Router

(USENIX Security 2004)

Tor

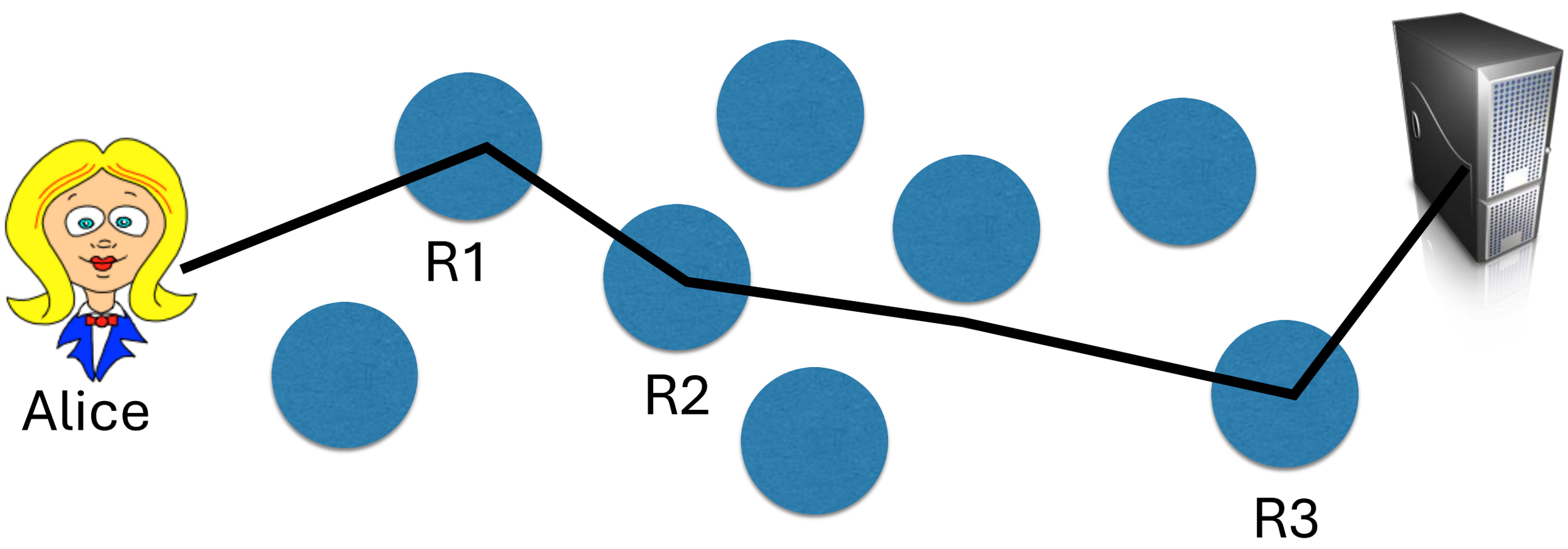
- Improved onion routing [we shall see how]
- Founded by US Navy Research Lab
- Designed for anonymous Web access
    - E.g., to allow US Navy officers to safely access navy servers when traveling abroad.
- Operational since 2003
- Very popular: ~8000 relays in late 2024

Circuit building in Tor

- Crypto suboptimality in OR: no forward secrecy.
  - Long term PK is used to encrypt secret keys
  - Tor introduced a “telescoping” key exchange protocol to establish pairwise symmetric keys between sender & hops.

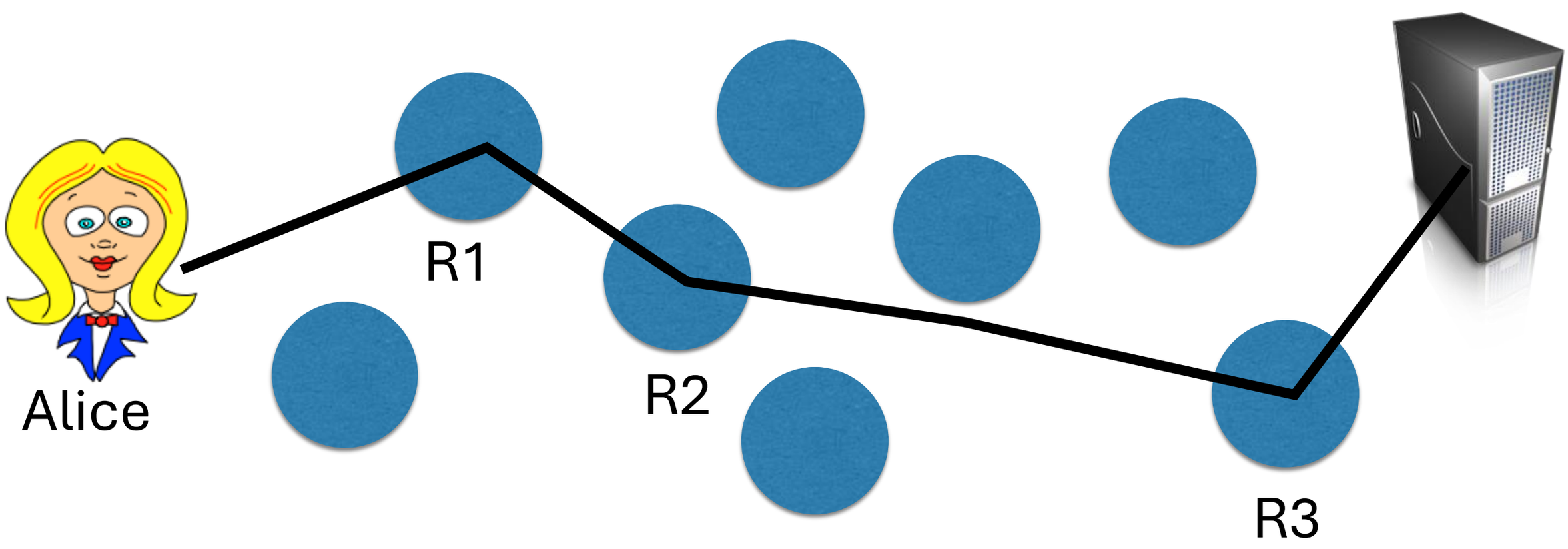
Circuit building

- Alice picks her path (say R1, R2, R3)
- Goal: establish three key between (Alice, R_j) for j=1,2,3
- Called **Entry Guard**, middle relay, and **Exit**



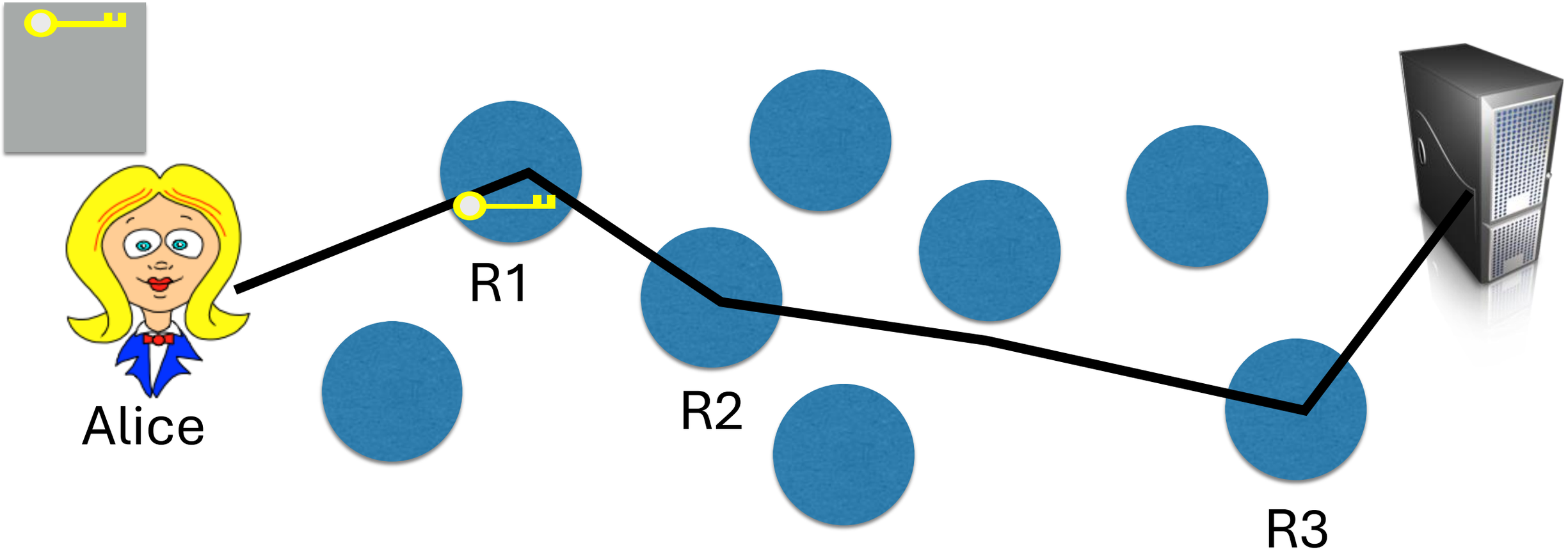
Circuit building

- Alice picks her path (say R1, R2, R3)
- Goal: establish three key between (Alice, R_j) for j=1,2,3
- Question: How about let Alice perform AKE with R1, R2, and R3 directly?



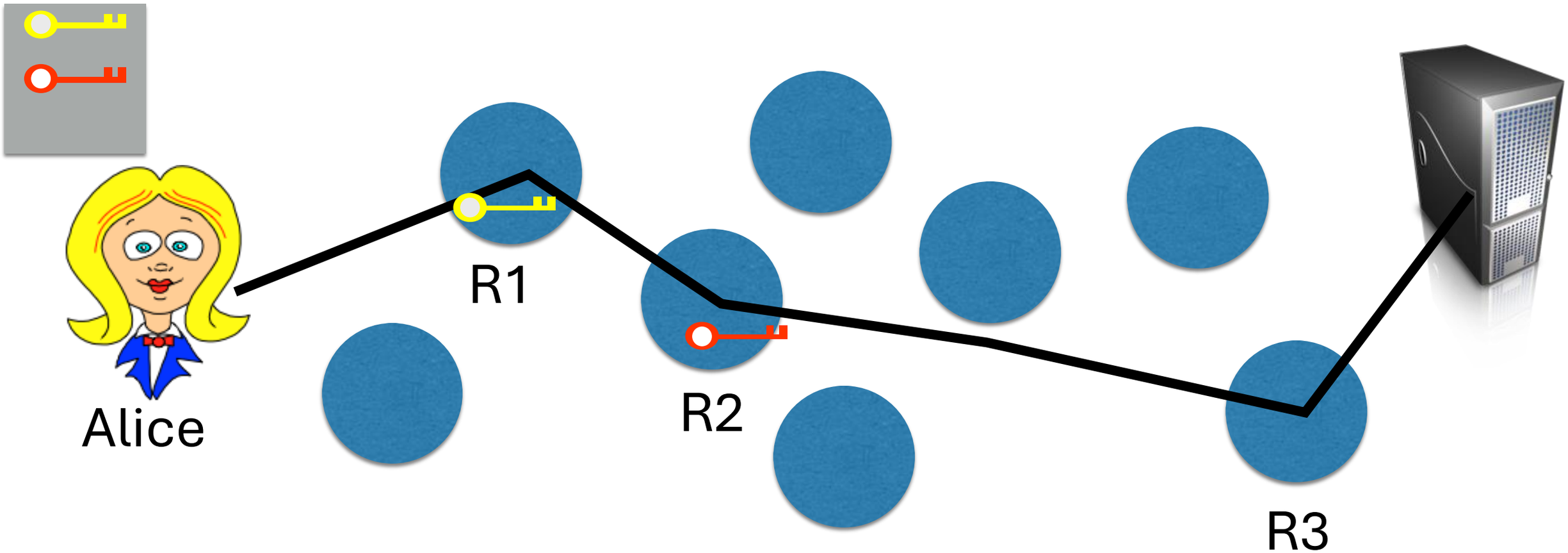
Circuit building

Alice performs AKE with R1



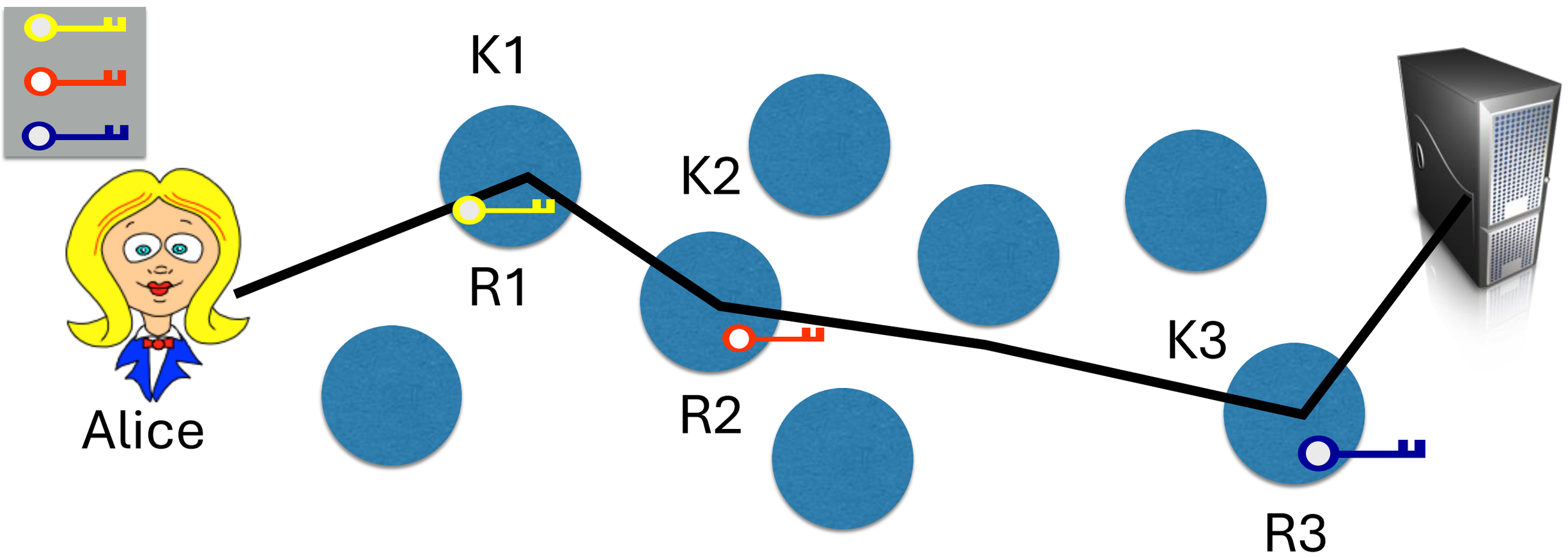
Circuit building

Alice performs AKE with R2, **tunneling through R1**



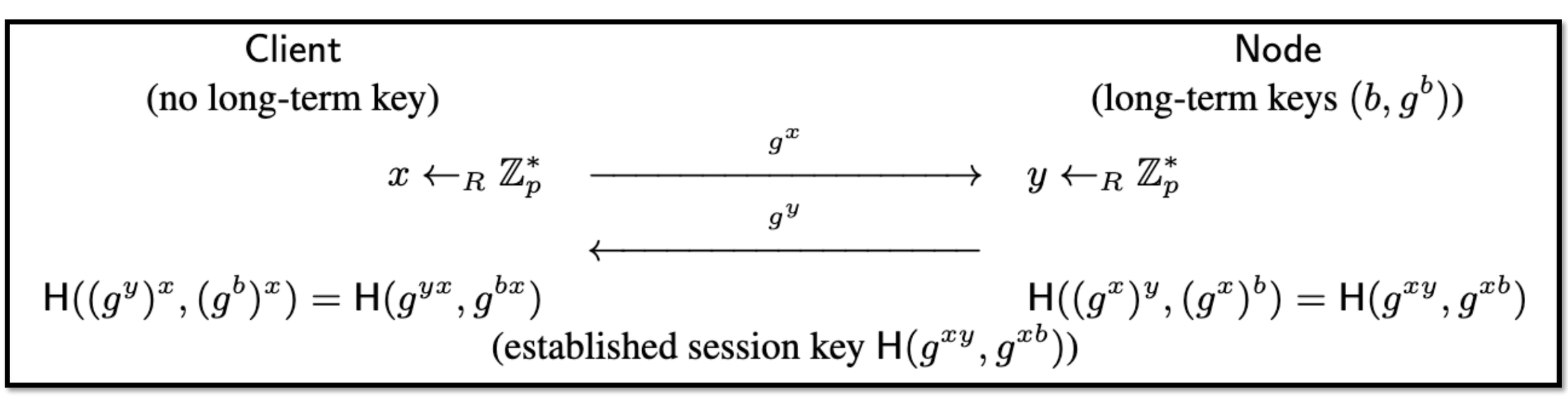
Circuit building

- And so on…
- In the end: Alice obtains pair-wise keys with each hope on the circuit
- Each router learns only the identity of the **previous** and **next** hops.



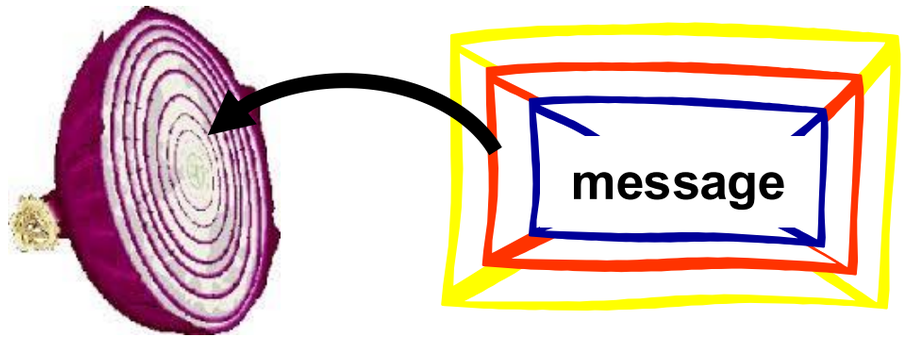
Tor’s AKE

- Latest Tor software uses a one-way AKE called NTOR



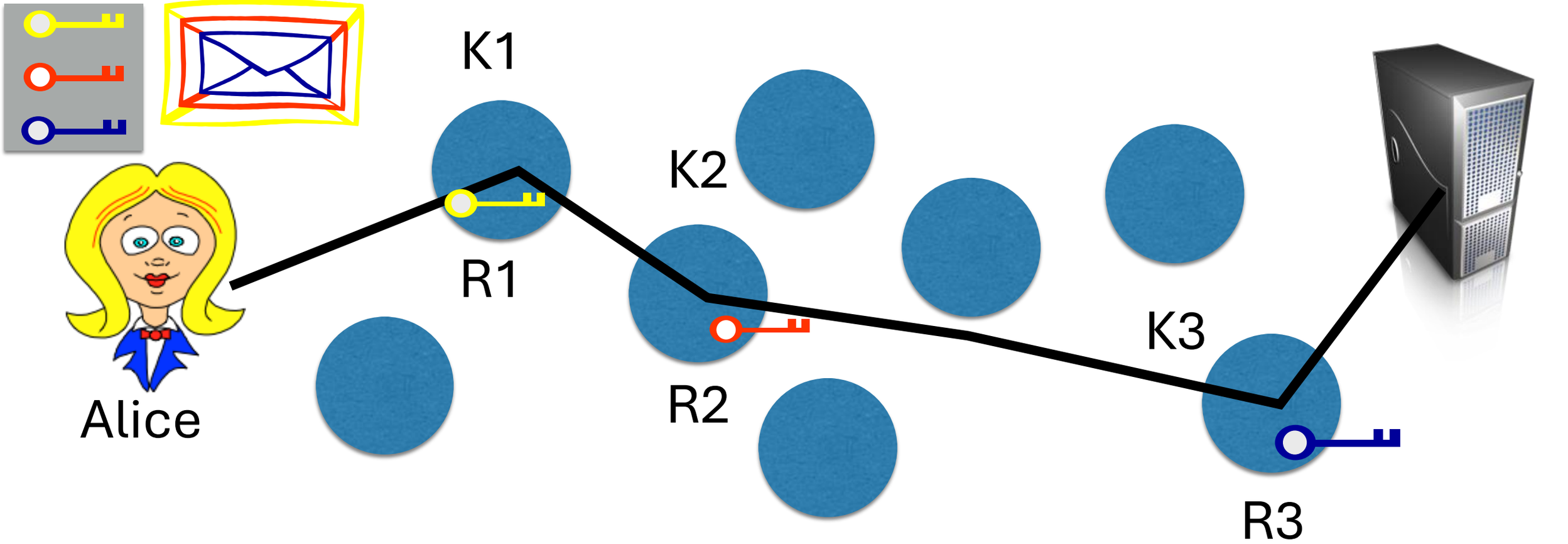
See “Anonymity and one-way authentication in key exchange protocols” by Goldberg et al. in 2013

Using the circuit

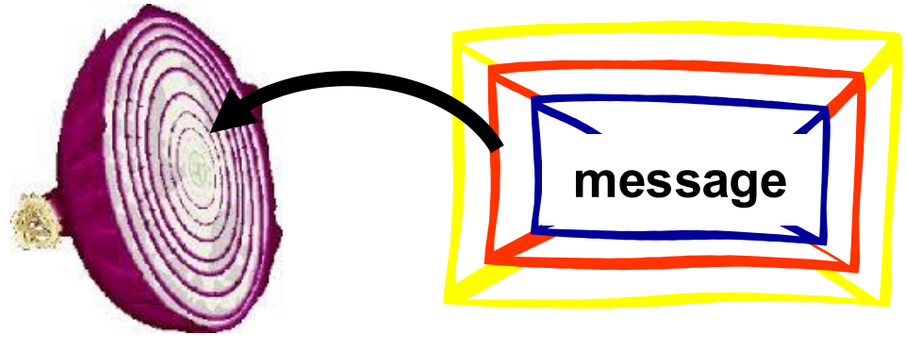


Onion (cell) =

$Enc_{K1}[Enc_{K2}[Enc_{K3}[\boldsymbol{m}]$,"Forward to R3"],"Forward to R2"]

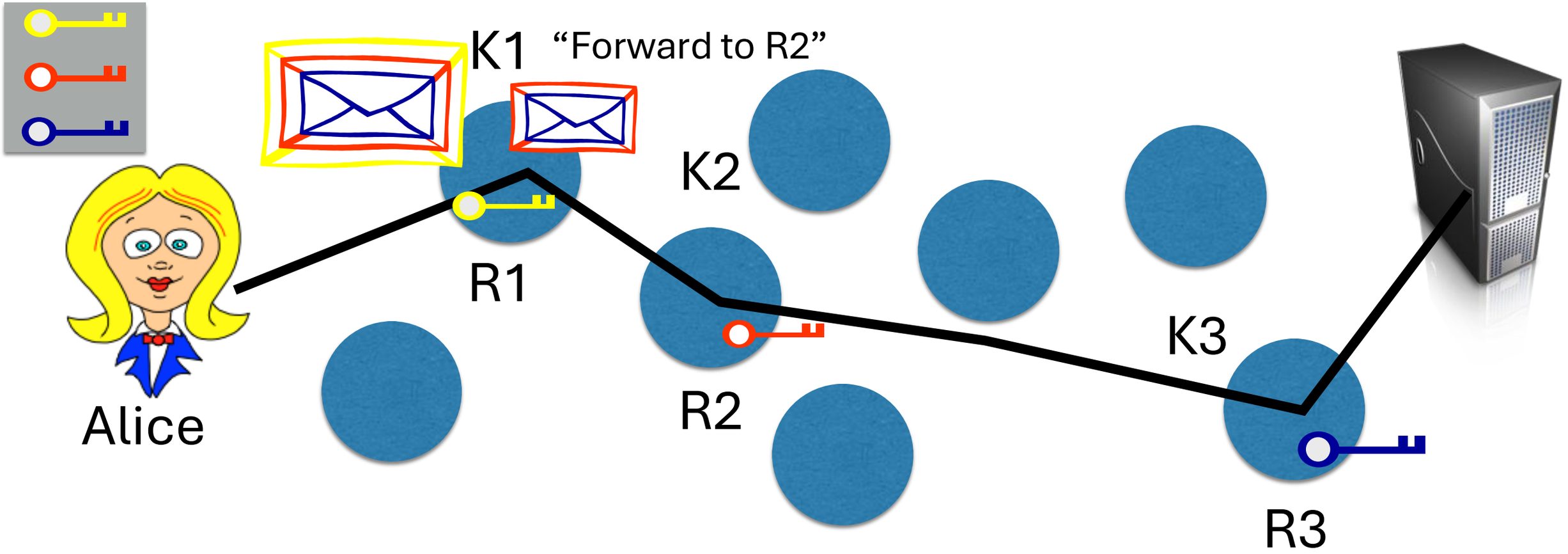


Using the circuit

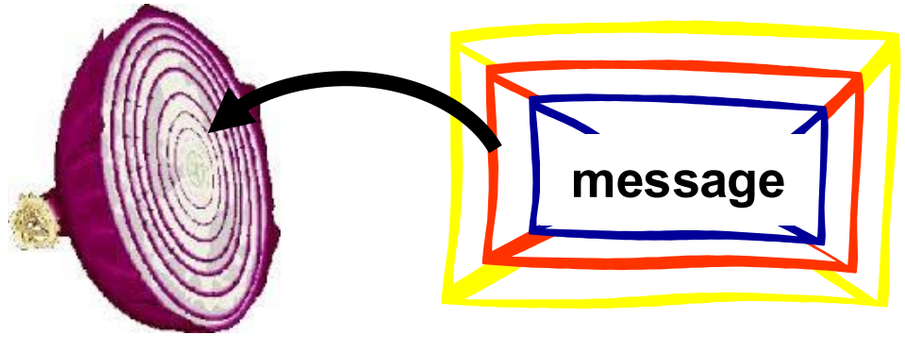


Onion (cell) =

$enc_{K1}[enc_{K2}[enc_{K3}[\boldsymbol{m}],$“Forward to R3”$],$“Forward to R2”$]$

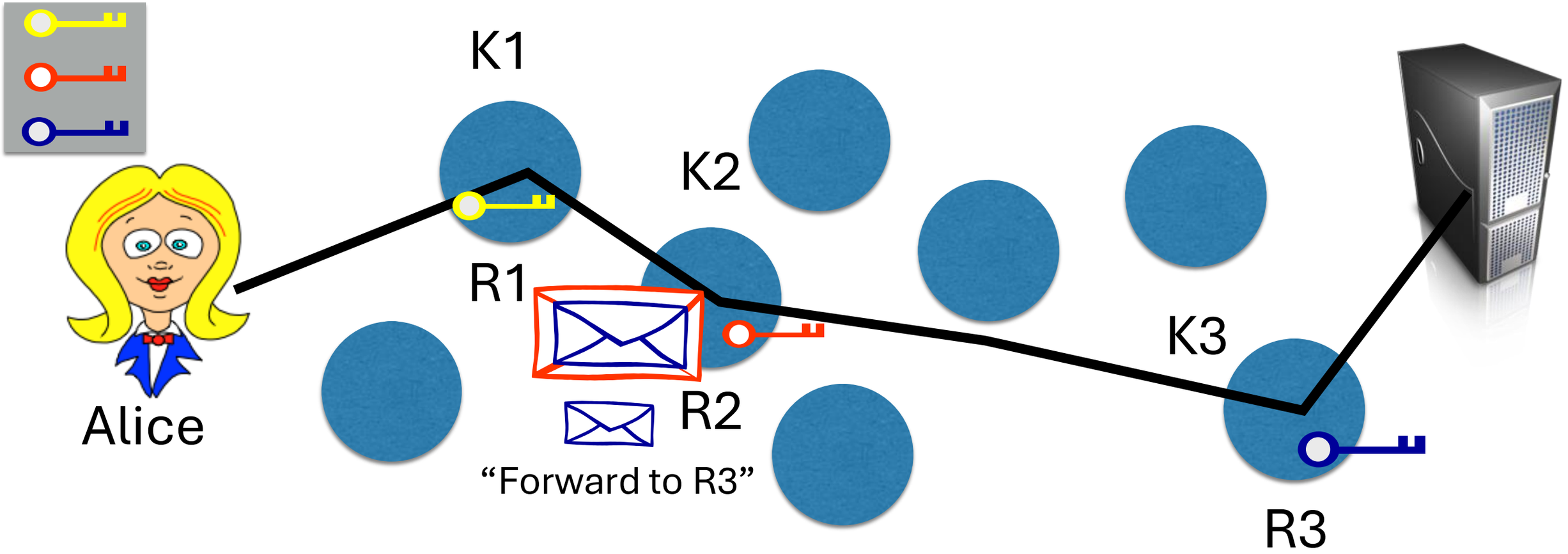


Using the circuit

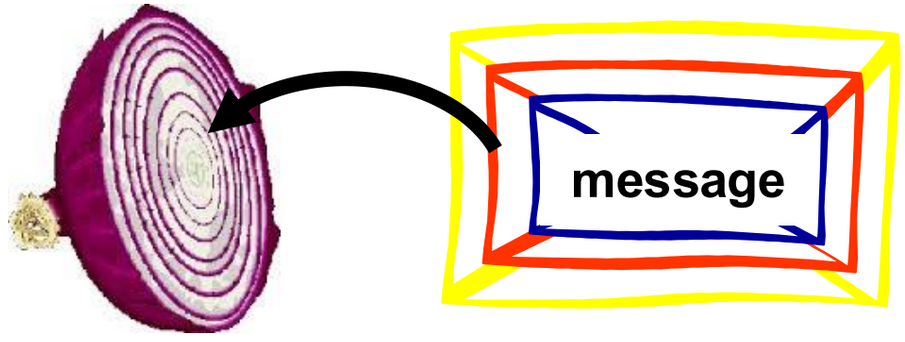


Onion (cell) =

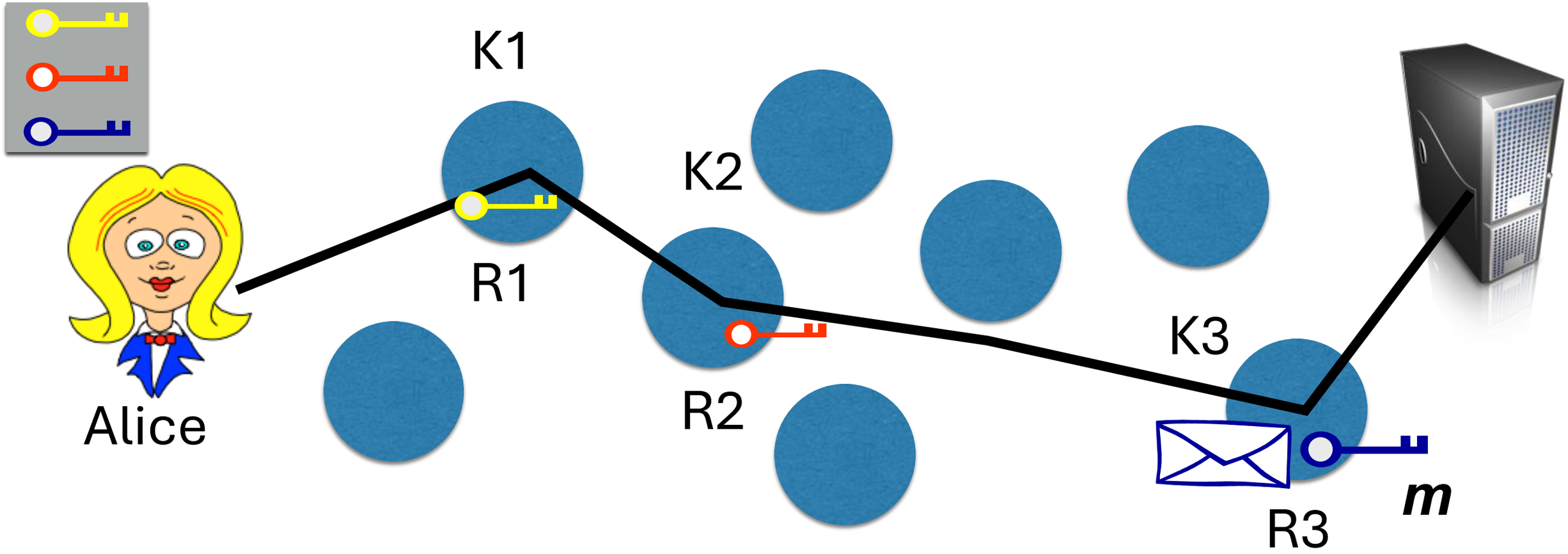
$enc_{K2}[enc_{K3}[\boldsymbol{m}],$“Forward to R3”]



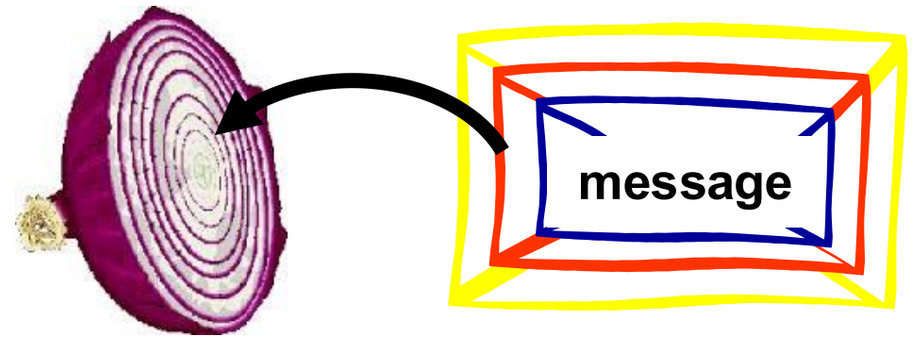
Using the circuit



Onion (cell) =
$enc_{K3}[\boldsymbol{m}]$

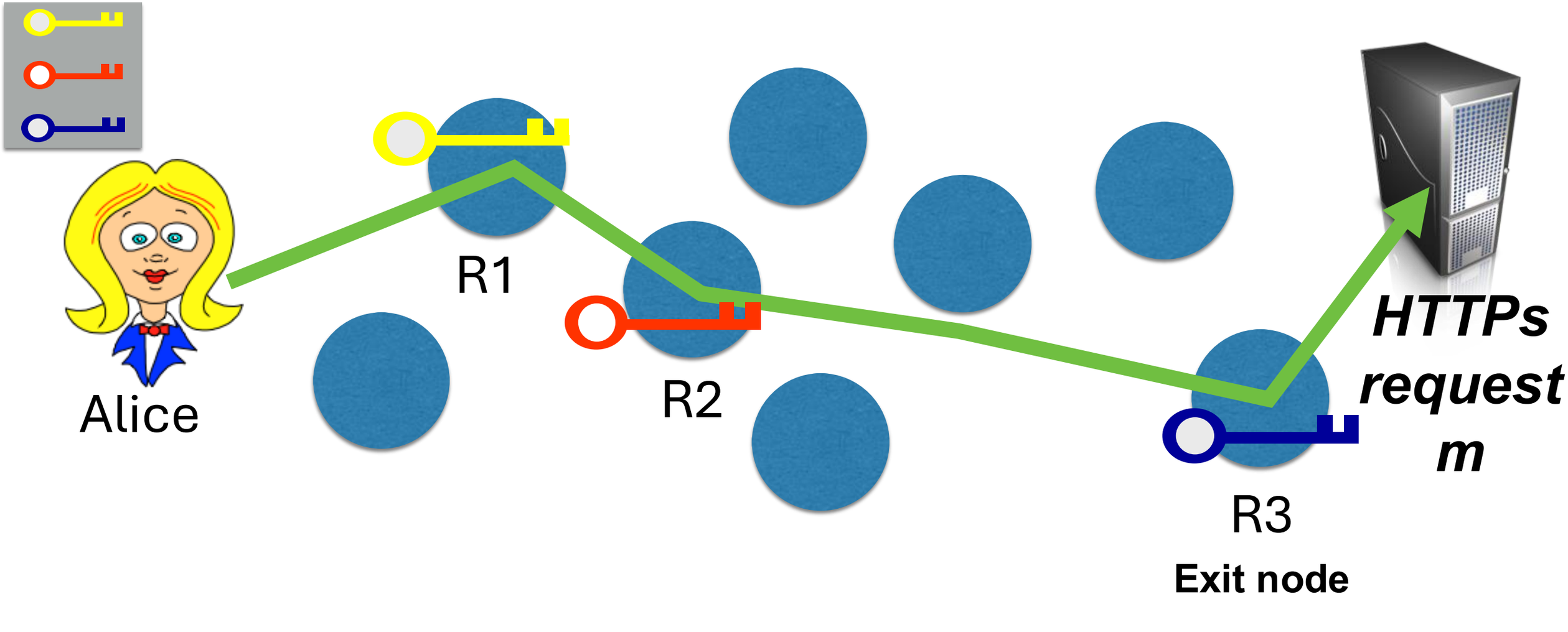


Using the circuit

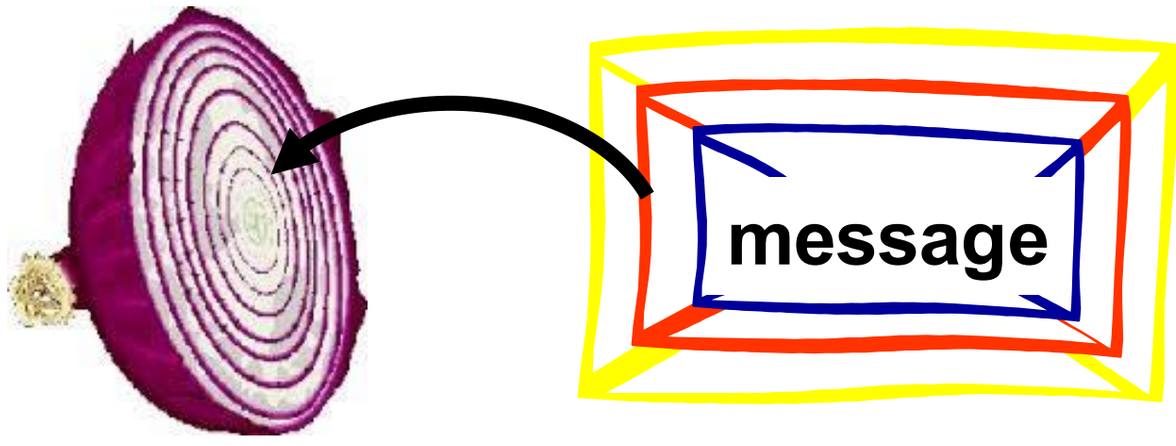


Note: server doesn't need to know Tor.

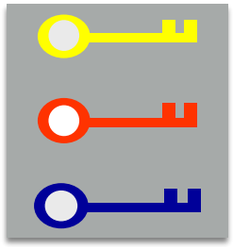
m is output!



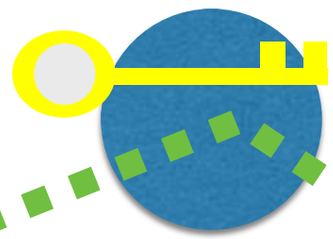
Using the circuit



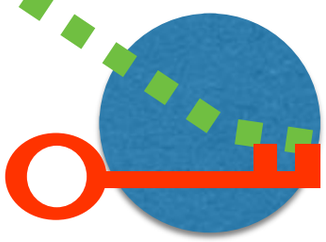
- How to handle response?
- Onion *built up* as return message passes along circuit



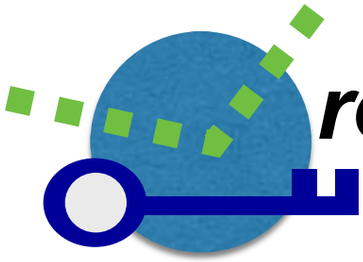
Alice



R1



R2

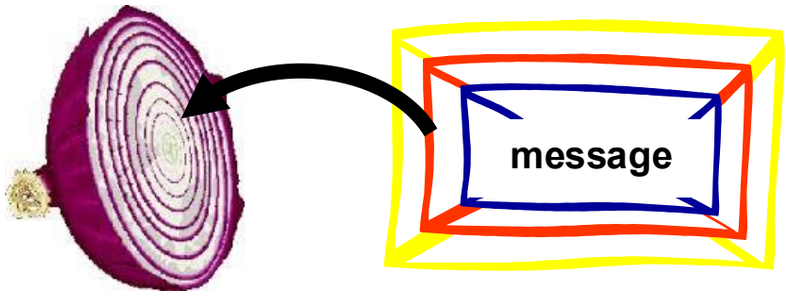


R3

Exit node

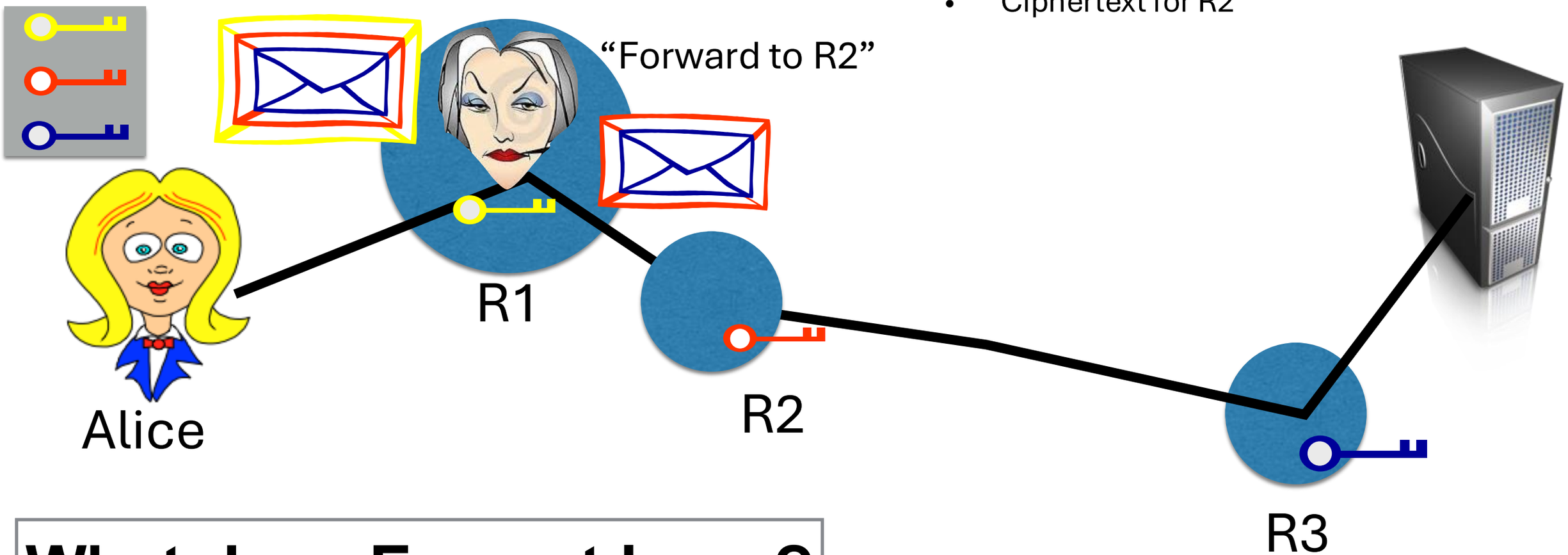
HTTPS response

View of the adversary



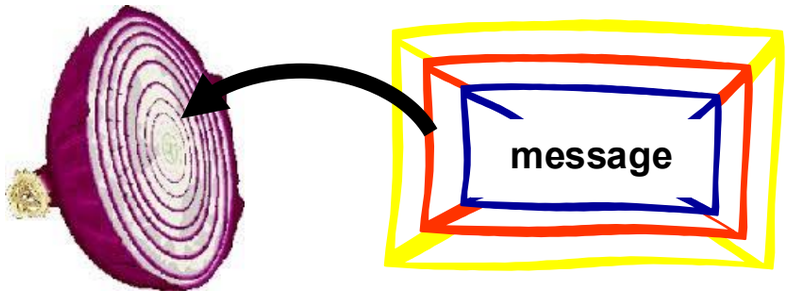
Suppose Eve compromises R1 (“entry guard”)

- Alice’s IP address
- R2 (“Forward to R2”)
- Red envelope
- Ciphertext for R2



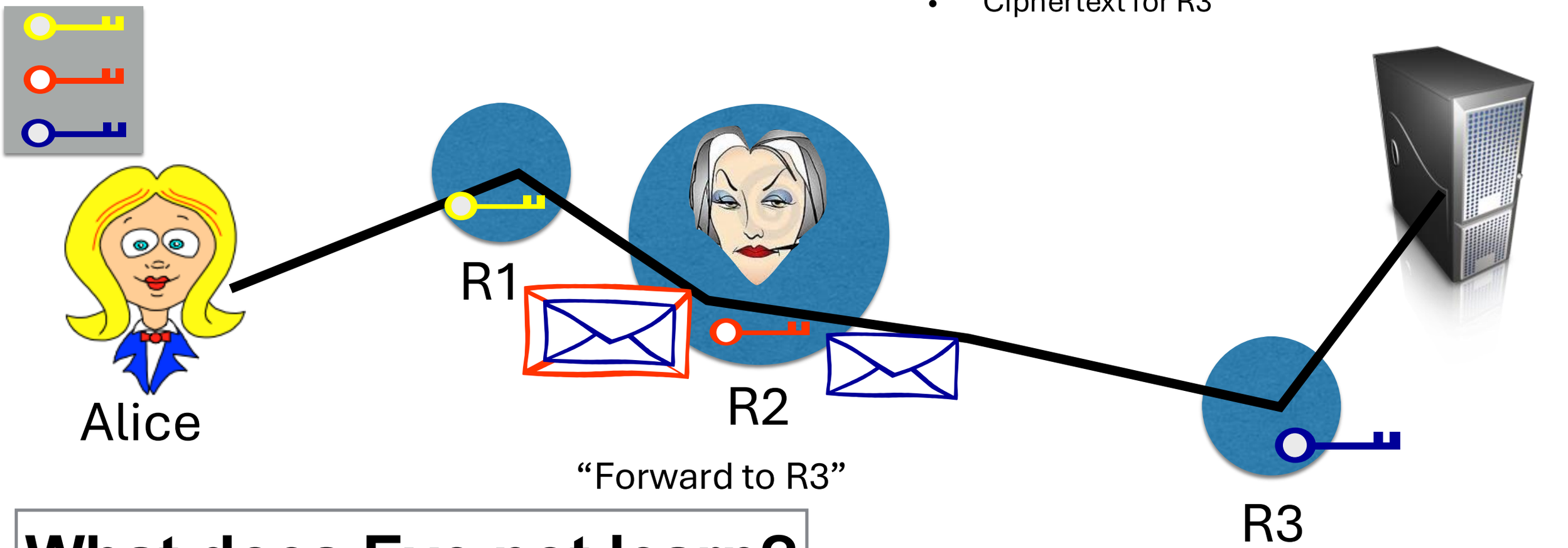
What does Eve not learn?

View of the adversary



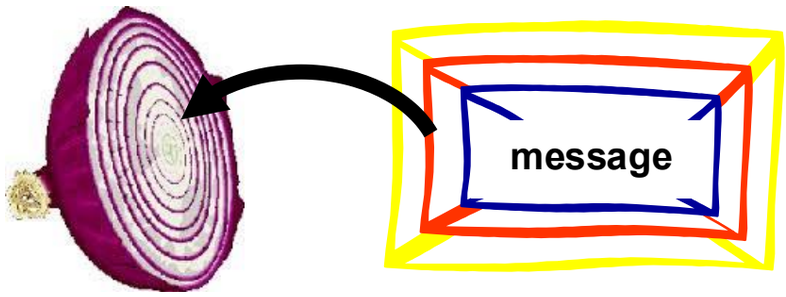
Suppose Eve compromises R2

- R1 (via IP address)
- R3 (“Forward to R3”)
- Blue envelope
- Ciphertext for R3



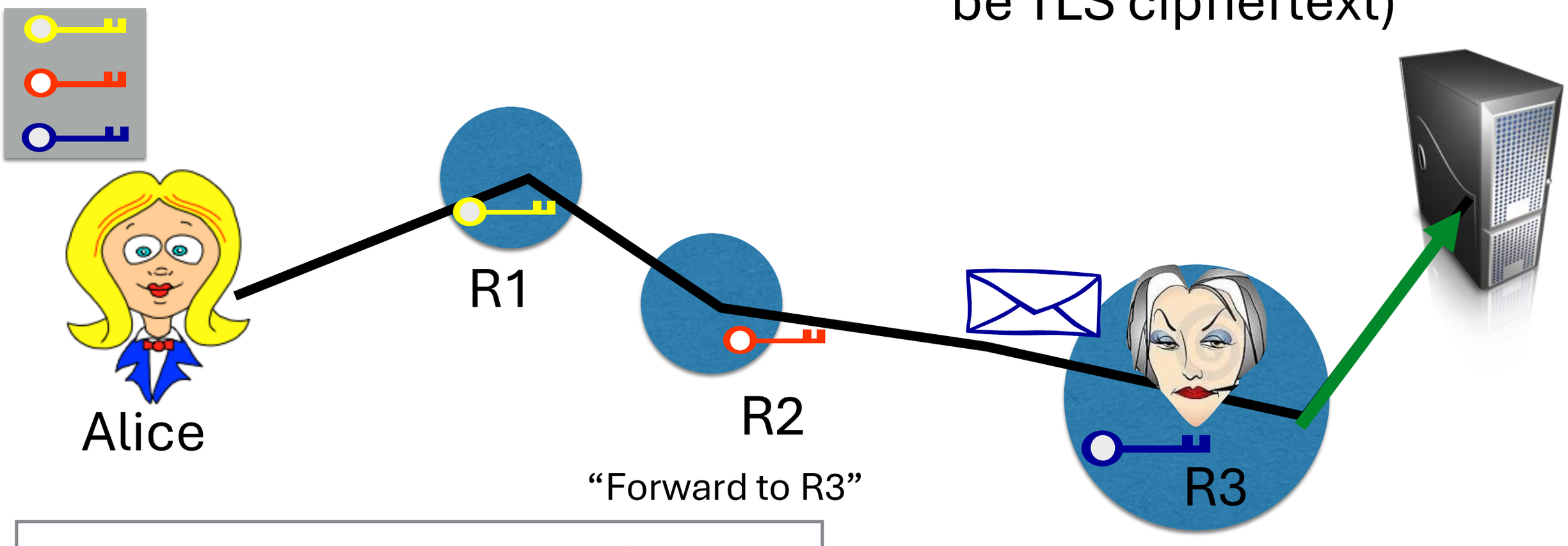
What does Eve not learn?

View of the adversary



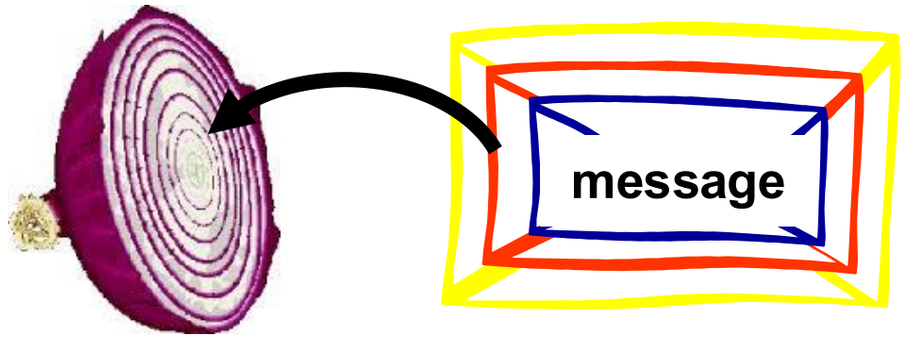
Suppose Eve compromises R3 (“exit node”)

- R2 (via IP address)
- Destination server
- Message *m* (Could be TLS ciphertext)

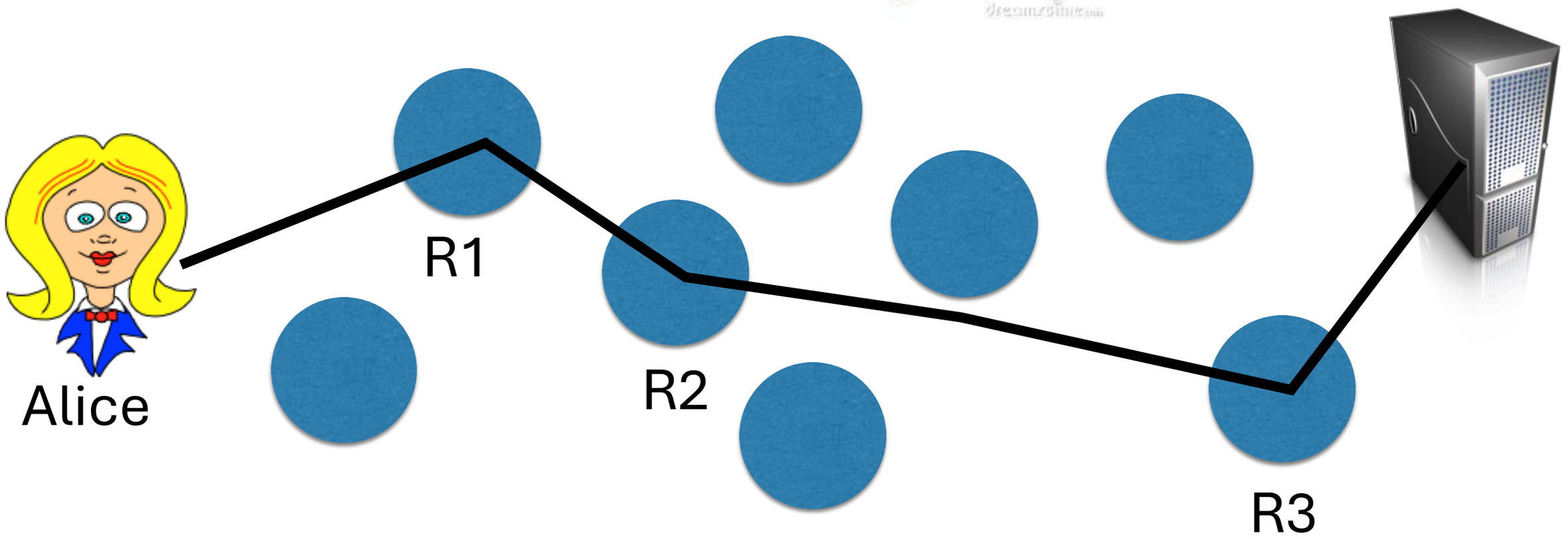


What does Eve not learn?

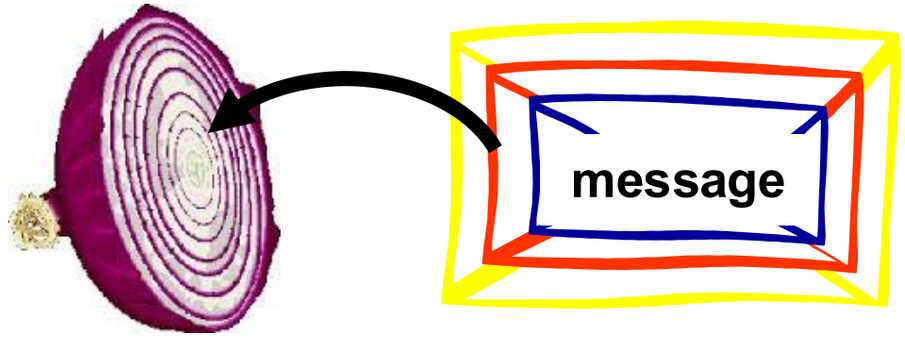
What if Eve sees *all traffic?*



Eve sees



But mixed in with...



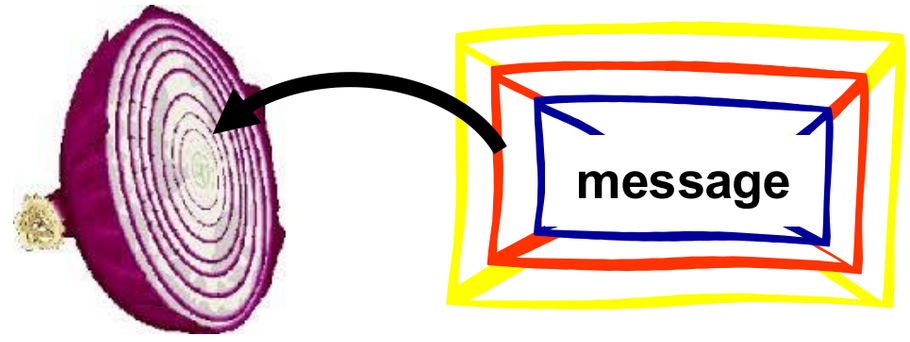
Charlie

Eve sees

Alice

Bob

So is Alice's circuit this?



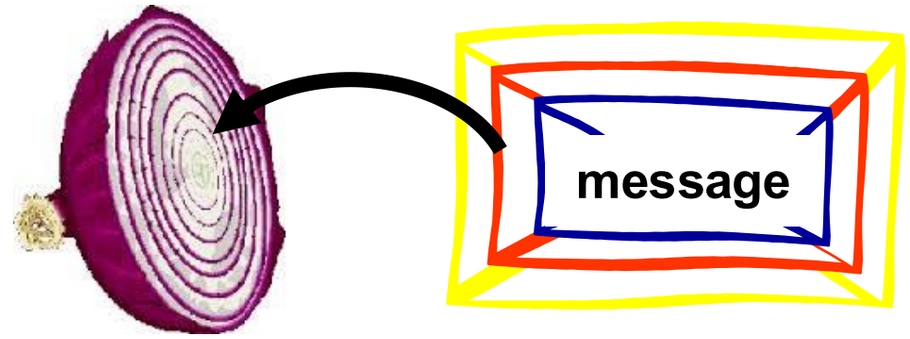
Charlie

Eve sees

Alice

Bob

Or this?



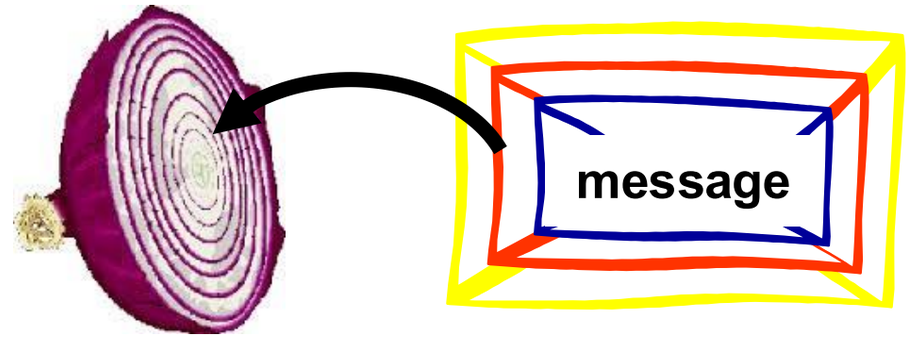
Charlie

Eve sees

Alice

Bob

Or this?



Charlie

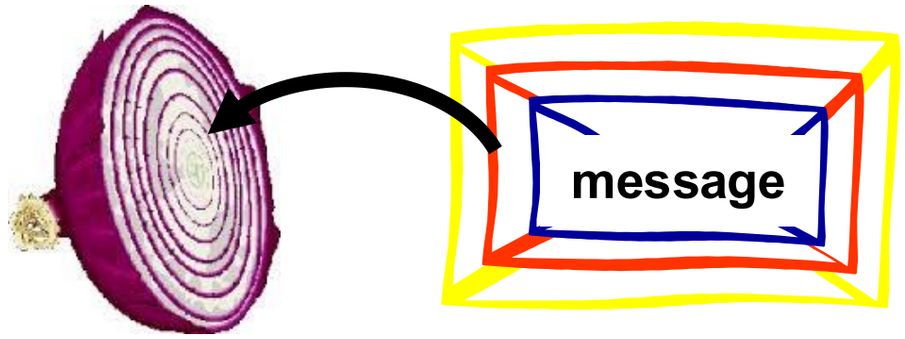
Eve sees

Alice

Bob

Still some attacks

...even if Eve controls only R1 and R3



- Timing
- Traffic volume

Charlie

Eve sees

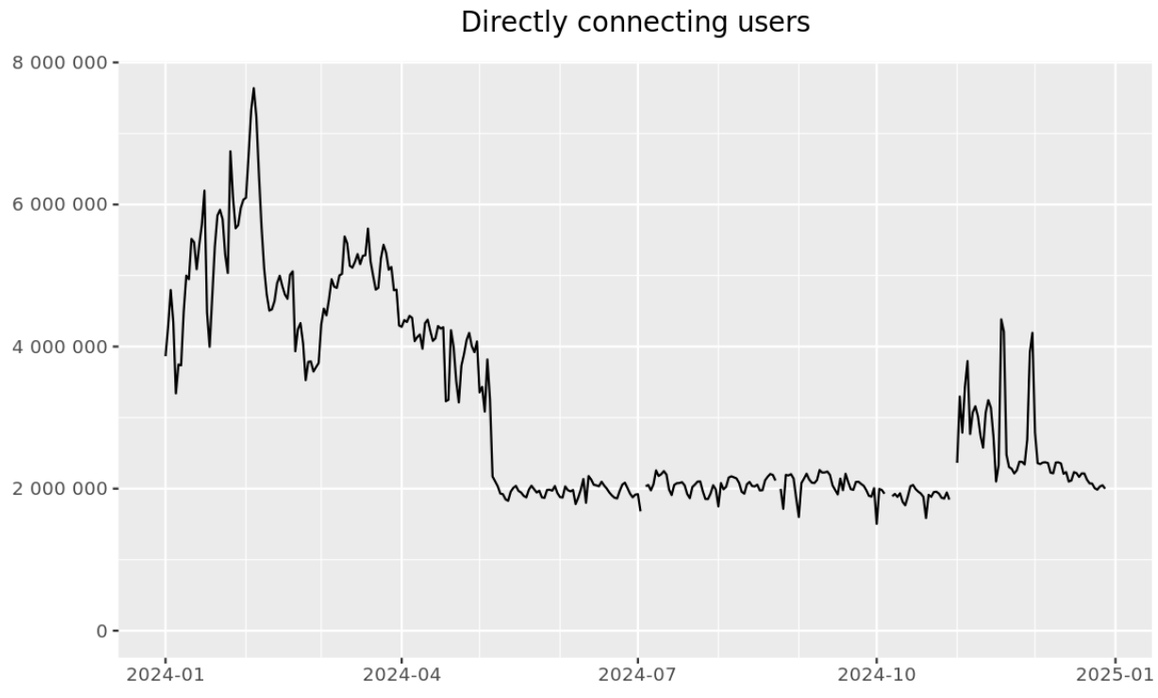
Alice

Bob

“Individualistic usage” v.s. anonymity

Tor is very popular!

- In use since 2003
- 10,000 relays (including bridges)
- Developed for U.S. Navy, but in use today by, e.g.,
  - U.S. Navy
    - Open source intelligence gathering
  - Journalists
    - Contact with dissidents and whistleblowers
  - Women’s shelters
    - Evading cyberstalking by abusers
  - Non-governmental organizations (NGOs)
    - Connection to home website without revealing activities to repressive governments
  - Hidden Services



Not very popular in China

The anonymous Internet

Daily Tor users per 100,000 Internet users

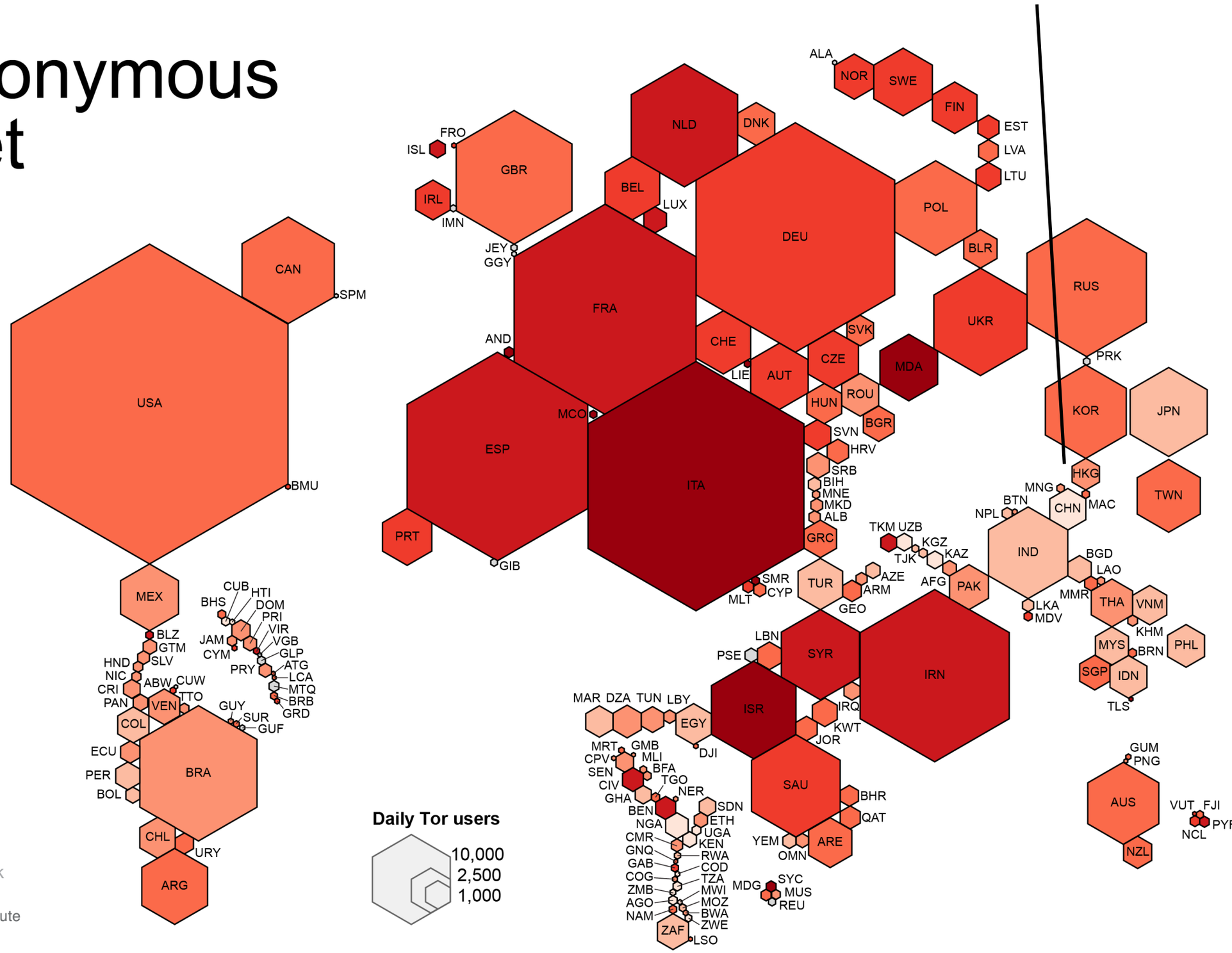
- > 200
- 100 - 200
- 50 - 100
- 25 - 50
- 10 - 25
- 5 - 10
- < 5
- no information

Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk

Oxford Internet Institute
University of Oxford



Daily Tor users

10,000
2,500
1,000

Censorship v.s. anonymity

- How do an attacker's objectives differ between censorship and traffic analysis?
- What part of Tor designs may enable censorship?
- Distinct traffic pattern
  - For instance, in 2012, China and Ethiopia deployed deep packet inspection to detect Tor traffic by its uncommon ciphersuits
- Relay nodes are publicized so they can be blocked by state-controlled ISPs.

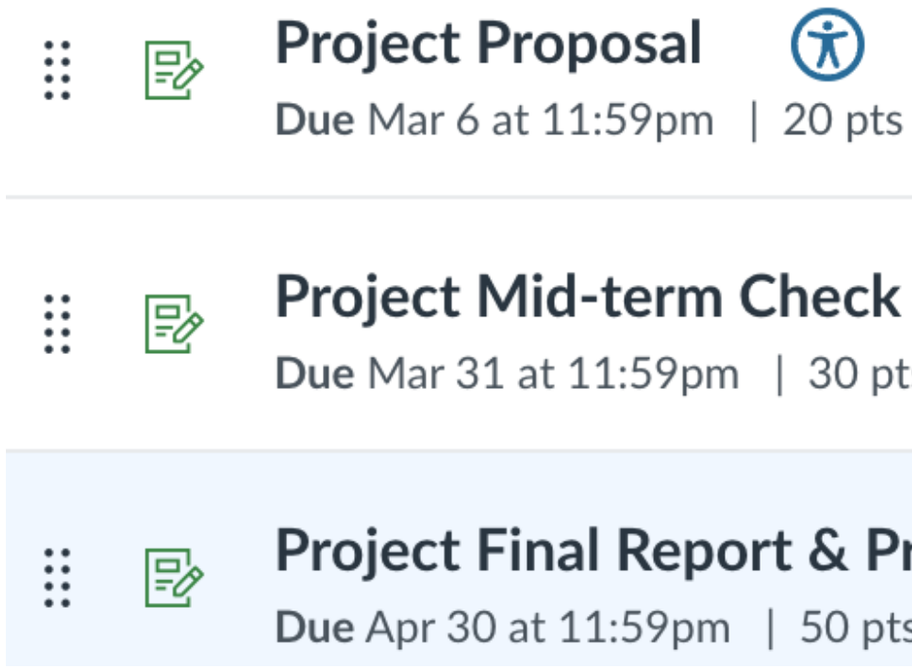
Announcements: First Paper Discussion Session coming up on Feb 23.

- Presentation order determined by SHA-256(rwc26, netid)
  - **Jerry Tan (jt2286)**
  - **Ben Merbaum (bpm36)**
  - brr32
  - mr2865
  - iwg3
  - rm2685
  - Ems264
- Everyone will get a chance.
- Pick your fav from the list. Walk us through the paper in 30 minutes.

13. (02-23) Presentations (two presentation by students):
    - Loopix (USENIX'17)
    - Attacking and Improving the Tor Directory Protocol (S&P'24, RWC'25)
    - Pudding: Private User Discovery in Anonymity Networks (S&P'24)
    - Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two (S&P'18)

Projects (Only applies to CPSC 5440)

- First Deadline in March (before spring break)



Goal & Success metrics

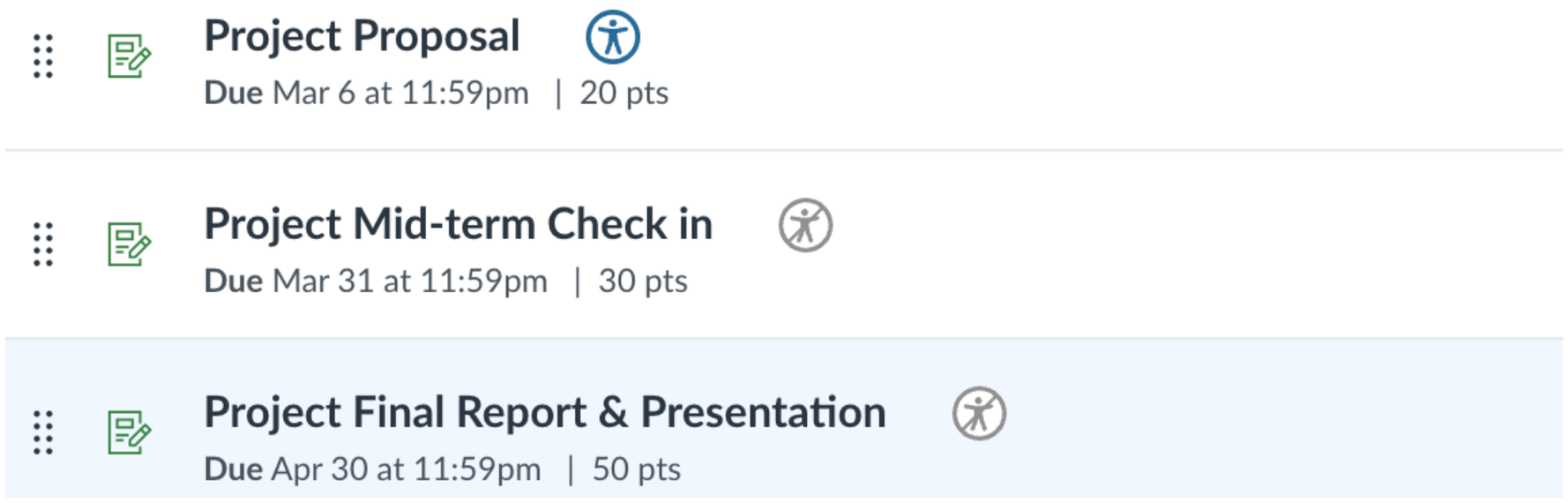
- The overall goal of the project is to dive into a ***specific* security-critical system** related to the course content, identify potential security gaps, and apply cryptographic tools to improve security.

- Two key metrics for success:
  - **Real-world Relevance**: Ideally, you work on a problem that affects a broad range of users and have strong societal impact.
  - **Novelty**: a successful project should contribute new knowledge to the area of real-world cryptography. Examples include: gaining a *new* understanding of a specific problem, identifying a *new* problem, and proposing a *new* direction to improve an existing solution.

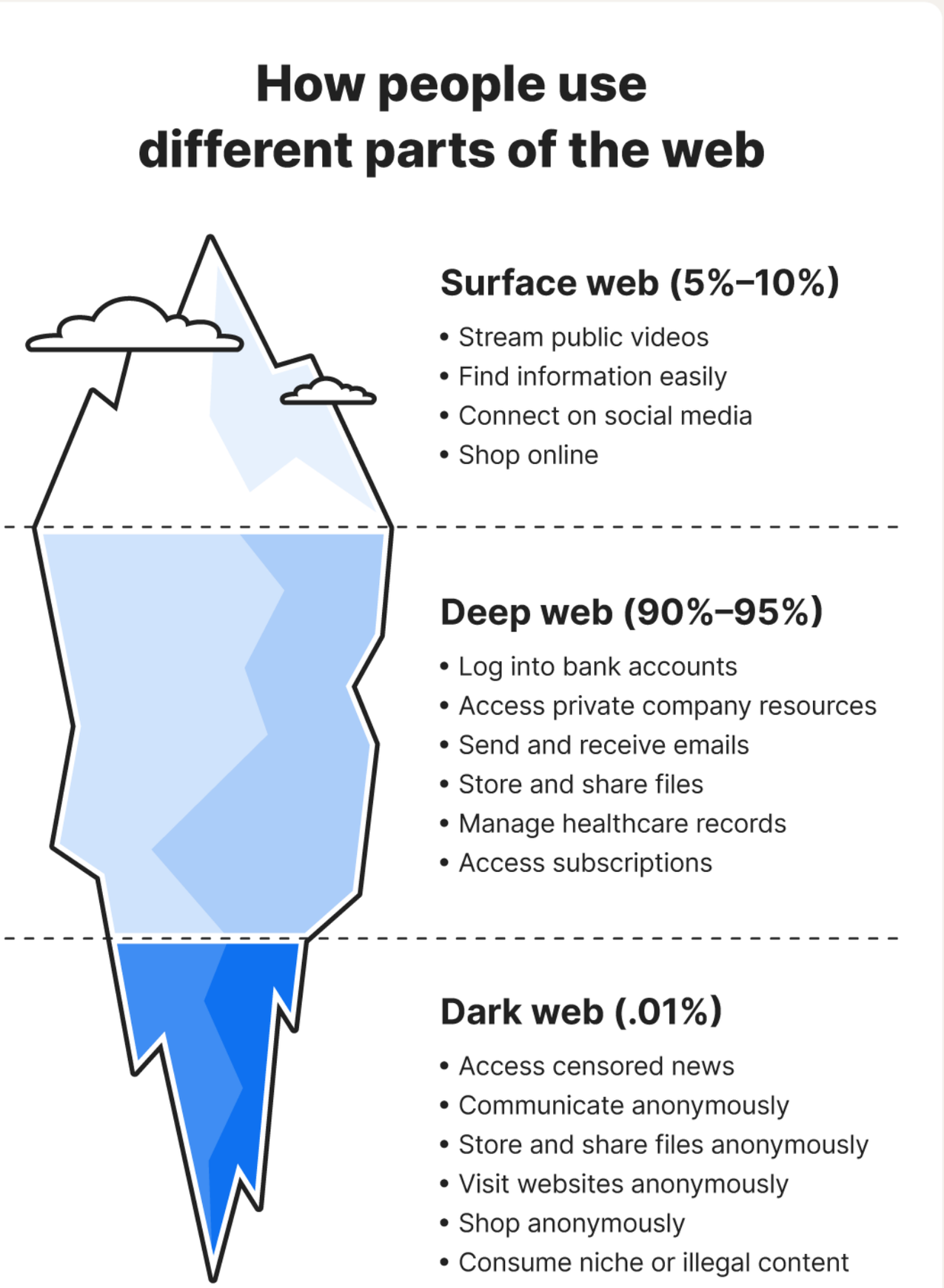
- You can work on any topic satisfying the above two requirements. Examples based on the content so far
  - Improving privacy in Certificate Transparency systems
  - Understanding real-world deployment of zkTLS systems
  - We will suggest topics in the lecture.

Milestones

- **Proposal**: 1-2 pages specifying the motivation, problem formulation (can be a sketch), related work, your methods, and your expected contribution. Importantly, also specify the deliverables by two milestones: the mid-term check-in (see below) and the final presentation.
- **Mid-term check-in (due end of March)**: 4-5 pages. Extending your proposal with mid-term deliverables. By this point, the problem should be sharpened and refined, and the potential of novelty and success should be clear.
- **Final report and presentation:** as long as it needs. You will present the results in the last lecture.



Hidden Services
a.k.a. the **Dark Web**



- **Surface web**: “everything google can scrape”
- **Deep web**: web content not publicly available
- **Dark web**: only accessible via anonymity networks

Key security requirements

- Regular web services must expose their **IP addresses** to be accessible.
- “Hidden” Services: publishing services w/o revealing the **IP addresses**.
- How to connect to something w/o an IP?

Positive uses of HS

https://securedrop.org/directory/

s of HS

Bloomberg Industry Group >

A platform with a news outlet focused on government, regulatory, legal and business news.

English, USA, business, civil liberties, crime, criminal justice, cybersecurity, environment, government, health, regulatory, social justice, technology

Bloomberg News >

Bloomberg News is an international news agency h

English, All countries, USA, business, government, te

Financial Times >

A UK daily business newspaper

English, Asia, Europe, UK, USA, business, civil liberti
cybersecurity, environment, government, health, hu
law enforcement, national security, social justice, te

Forbes >

Forbes is an American business magazine.

English, All countries, USA, business, cybersecurity, e
health, law enforcement, multimedia, national secu

New York Times >

The New York Times is an American newspaper bas

Chinese, English, Spanish, All countries, USA, arts, bu
government, health, science, sports, technology, trav

POLITICO >

A website covering politics and policy in Washington and beyond.

All languages, English, USA, business, government

Stefania Maurizi's Secure Drop Platform

Stefania Maurizi >

Italian investigative journalist with expertise on high-profile leaks and whistleblowers

All languages, English, French, Italian, Europe, Italy, UK, USA, civil liberties, corruption, cybersecurity, environment, government, human rights, inequality, law enforcement, national security, science, social justice, suppression of dissent, technology

The Guardian >

The Guardian is a British daily newspaper.

All languages, English, All countries, UK, USA, business, civil liberties, environment, government, health, national security, technology

The Intercept >

The Intercept is an online news publication dedicated to adversarial accountability journalism.

English, All countries, USA, business, civil liberties, criminal justice, environment, government, national security

The Washington Post >

The Washington Post is an American daily newspaper published in Washington, DC.

https://securedrop.org/directory/

The Guardian SecureDrop

Share stories with us securely and confidentially

How to access the Guardian's SecureDrop service

1. Download and install software to access the Tor network: https://www.torproject.org. For security reasons, we advise you, especially if you are uploading documents, not to use your home or work network, but instead to use a public Wi-Fi network in an area where your screen is not visible to security cameras. Alternately, you can start up your computer from a USB key loaded with the Tails secure operating system, which is available at https://tails.net and includes the Tor web browser.

2. Once you launch the Tor browser, copy and paste the URL **xp44cagis447k3lpb4wwhcqukix6cgqokbuys24vmxmbzmaq2** or **theguardian.securedrop.tor.onion** into the Tor address bar. When the page loads, you will find further instructions on how to submit files and messages to the Guardian.

3. You will be assigned a randomly generated and unique code phrase. If a writer or editor at the Guardian wants to contact you about the information you have submitted, they will leave a message for you in SecureDrop. The messages can only be accessed using your code name. These messages are the only way we will be able to reach you.

https://www.theguardian.com/securedrop. Feb 2026

Welcome | The Guardian | Secur

http://xp44cagis447k3lpb4wwhcqukix6cgqokbuys24vmxmbzmaq2gjvc2yd.on

Your Tor Browser's **Security Level** is too low. Use the button in your browser's toolbar to change it.

The Guardian

English

First submission

First time submitting to our SecureDrop? Start here.

GET STARTED

Return visit

Already have a codename? Check for replies or submit something new.

LOG IN

Powered by **SecureDrop 2.13.0**.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

Discussion

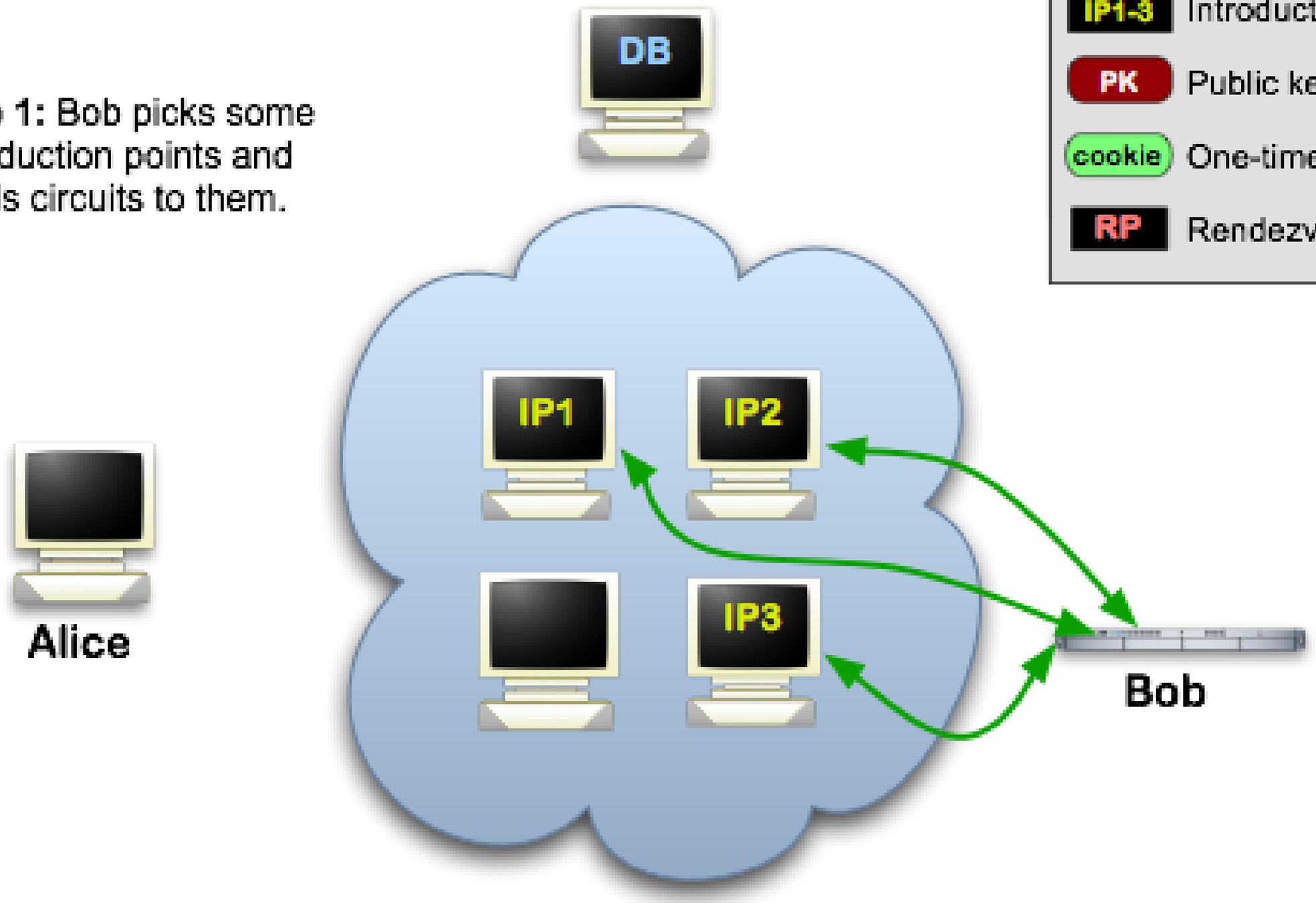
- Q: SecureDrop does not hide **identity**, only the **location**.

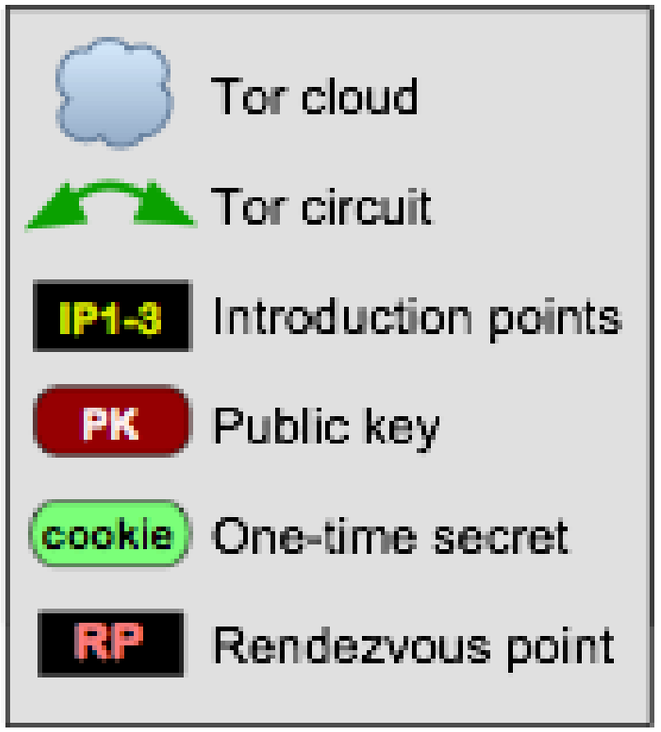
  Why is that useful?

- A: It reduces attack surface to a minimal.
  - Can’t block service by coercing Cloud service providers, ISPs, DNS providers, etc.
  - Taking down the service requires explicitly confronting the publisher.

Hidden Services: 1

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

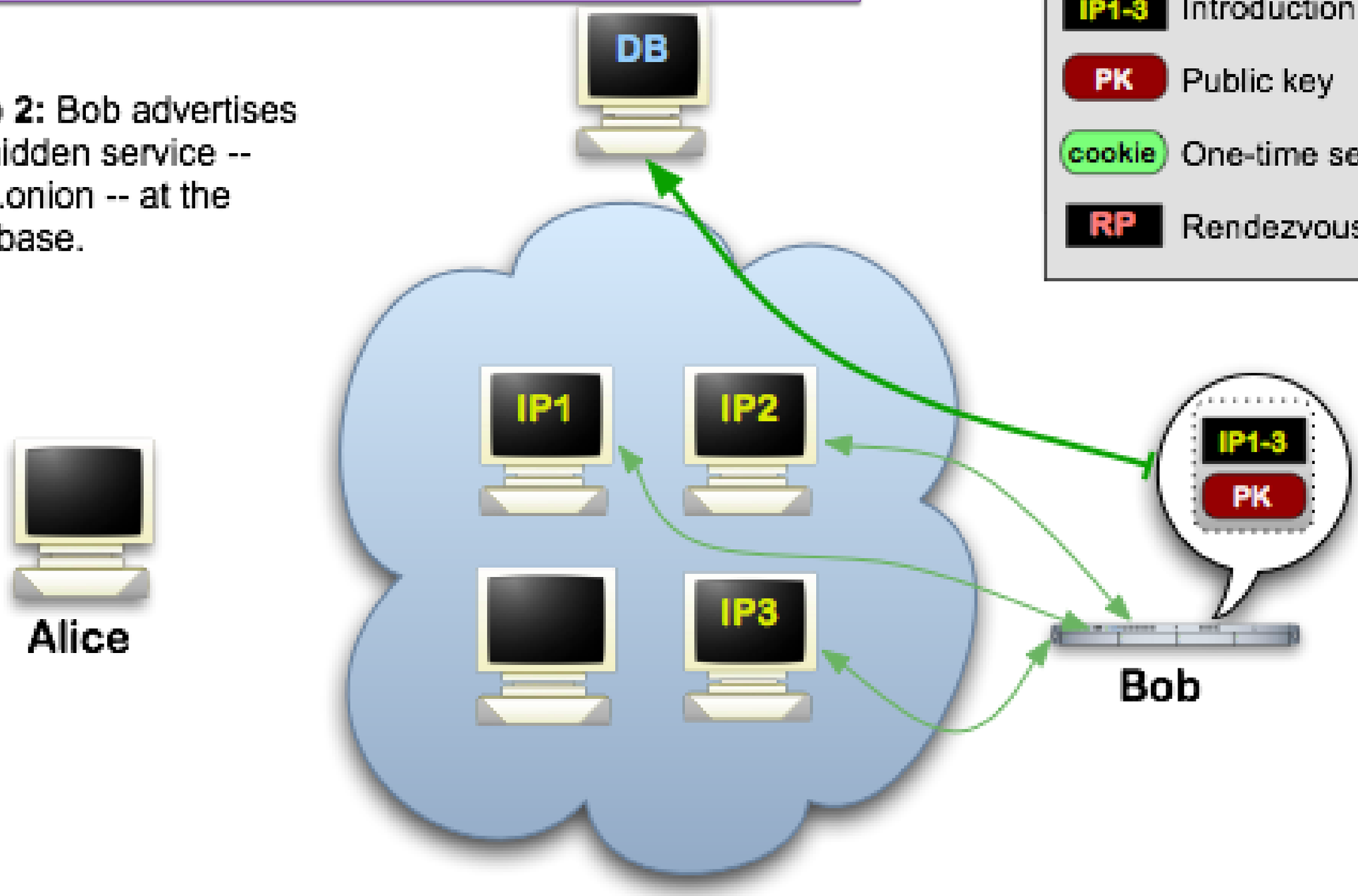


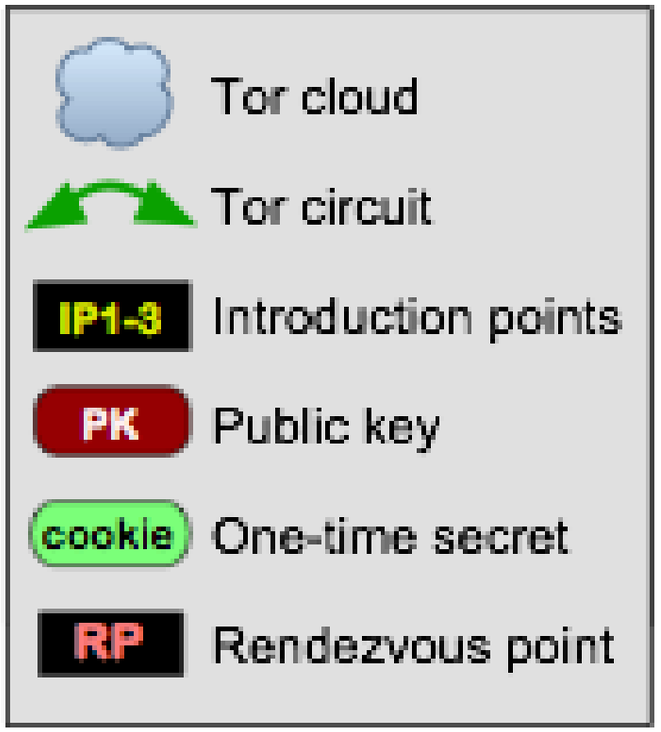


Hidden Services: 2

XYZ.onion: addresses of Intro Points

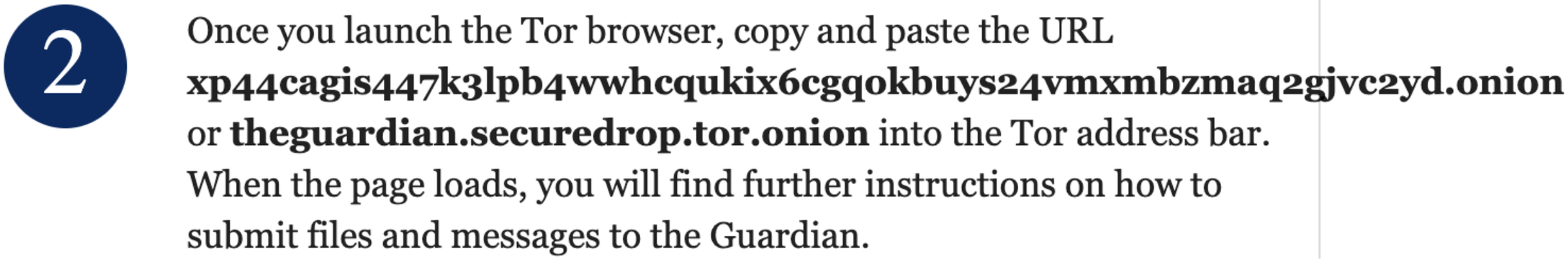
Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.





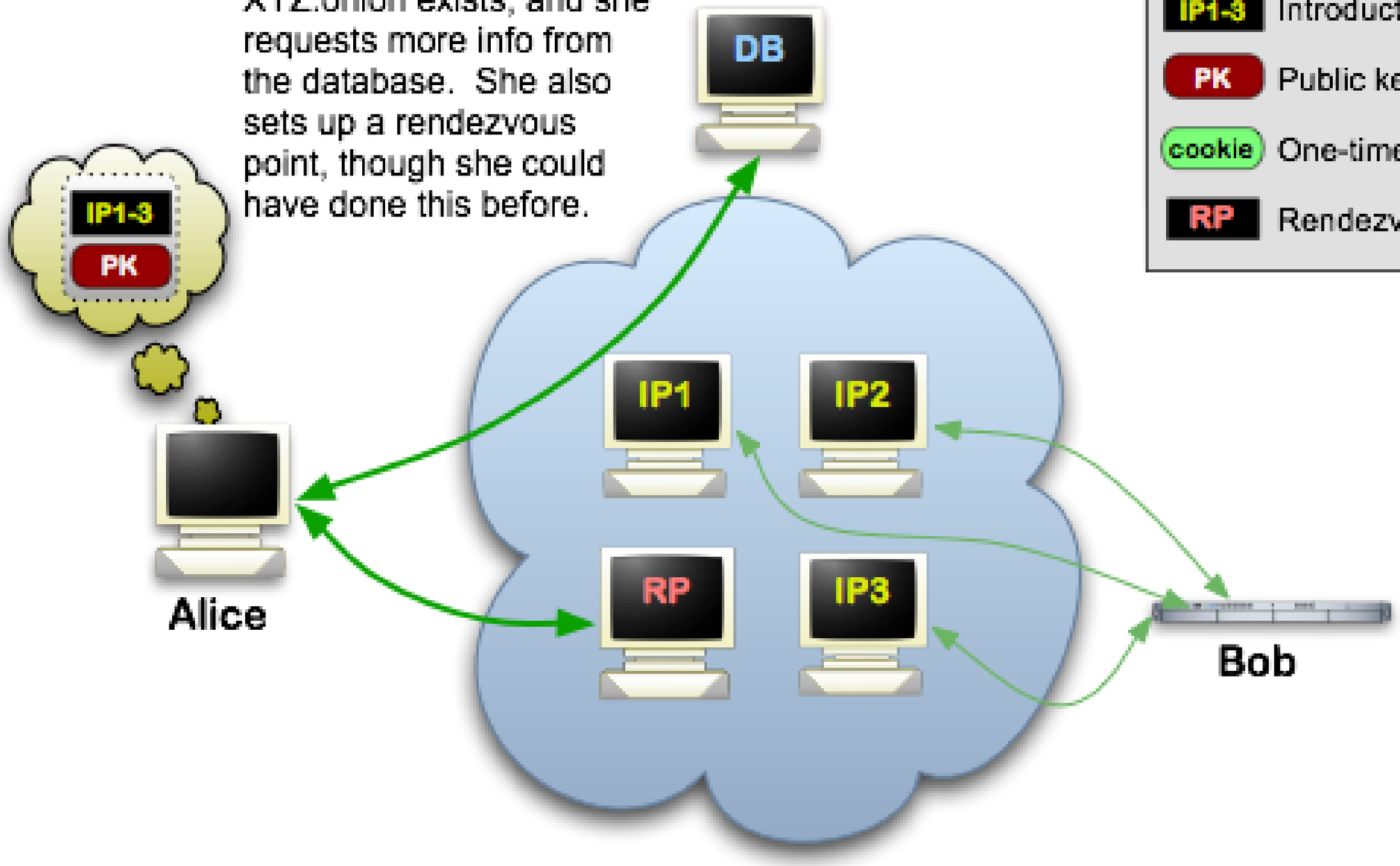
How do users discover HS?

- Typically out of band.
- E.g., SecureDrop links for The Guardian can be found at its regular website: https://www.theguardian.com/securedrop



Hidden Services: 3

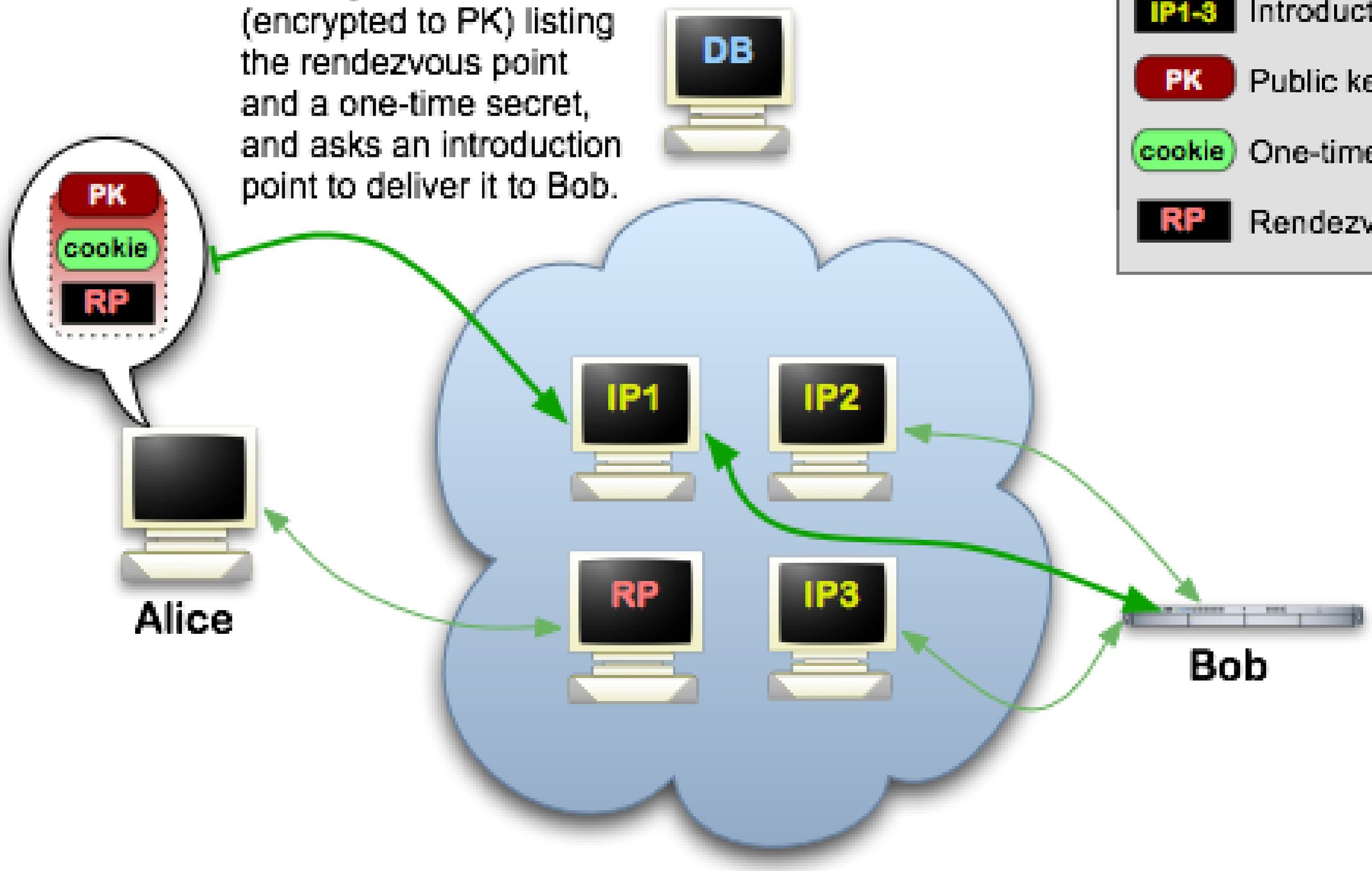
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



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

Tor Hidden Services: 4

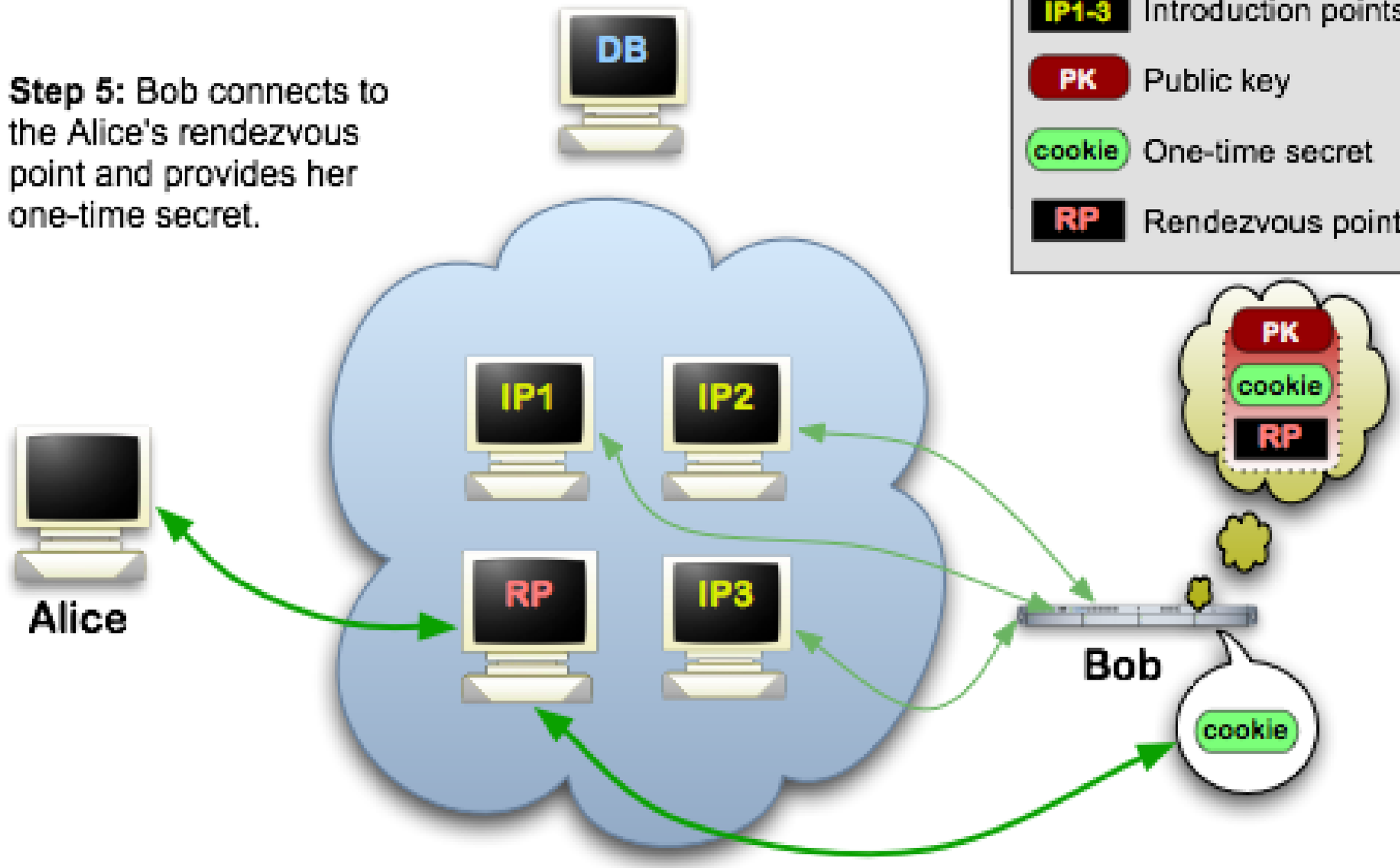
Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



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

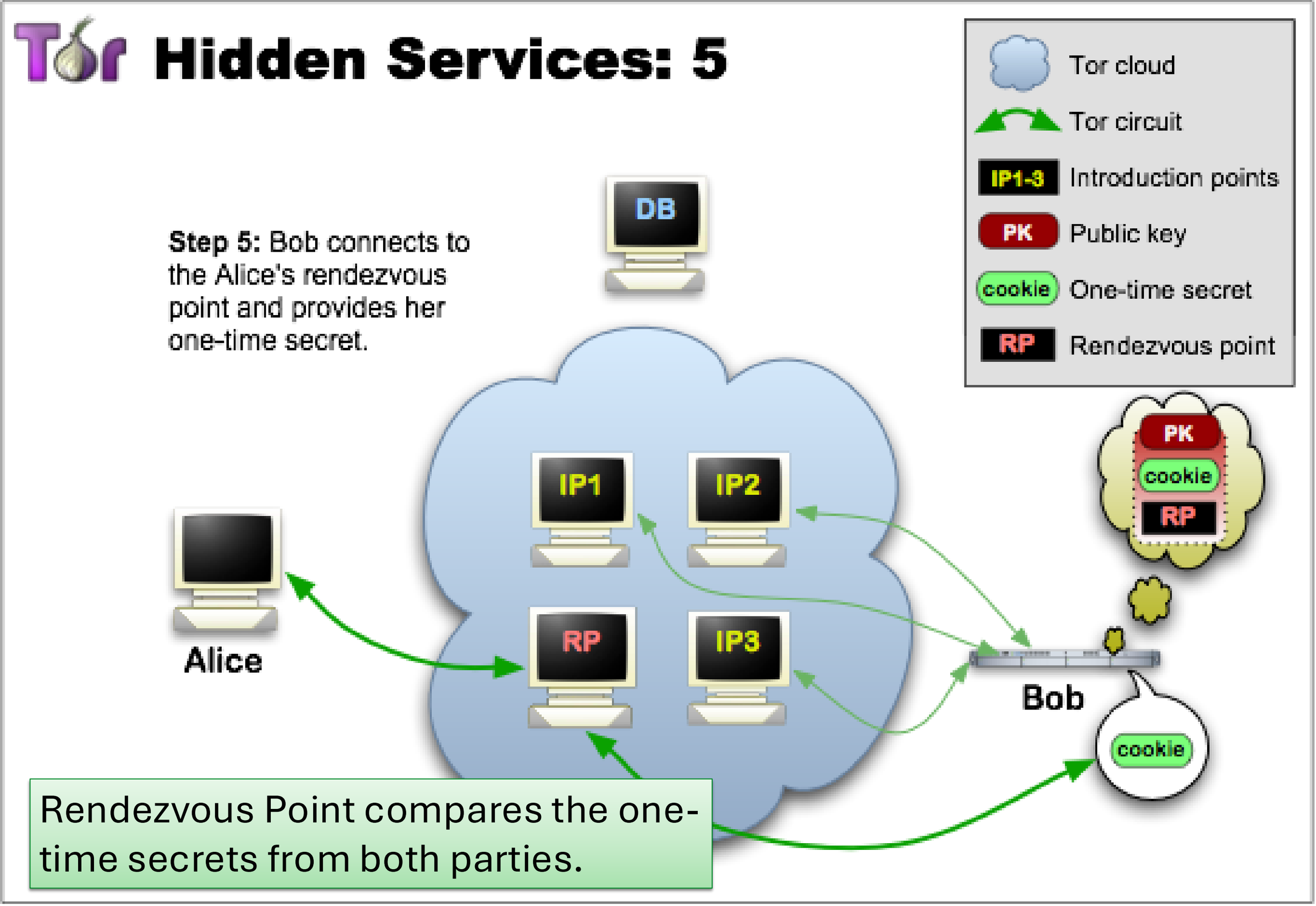
Hidden Services: 5

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



Hidden Services: 5

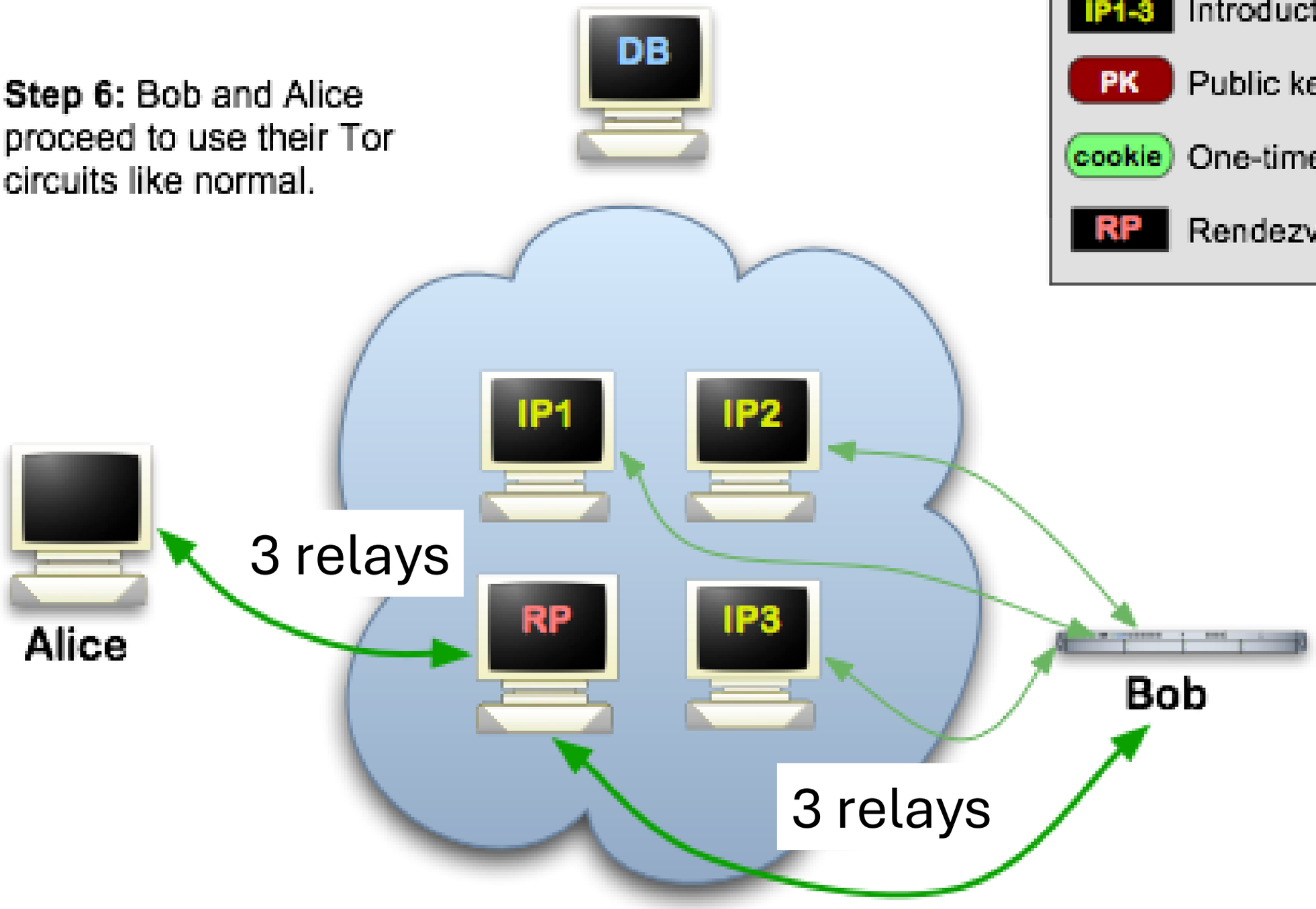
Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Caution: Bob’s IP address is known to the **entry guards**.

Hidden Services: 6

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



Tor cloud

Tor circuit

IP1-3 Introduction points

PK Public key

cookie One-time secret

RP Rendezvous point

Why don’t Alice and Bob communicate using intro point?

Welcome | The Guardian | Secur

http://xp44cagis447k3lpb4wwhcqukix6cgqokbuys24vmxmbzmaq2gjc2yd.on

Circuit for xp44ca...jvc2yd.onion

Tor Circuit

- This browser
- Moldova (guard) `176.123.1.217`
- Romania `62.133.45.2`
- France `62.210.222.112, 2001:bc8:32d7:1da::`
- Onion site relays
- xp44ca...jvc2yd.onion

New Tor circuit for this site
Your guard node may not change

Your

olbar to change it.

The Guard

sit

dename? Check
hit something

English

Powered by **SecureDrop 2.13.0**.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

Of course, use of Tor alone doesn’t guarantee anonymity

- Ulbricht arrested by FBI in Oct. 2013 and sentenced to double life imprisonment plus 40 years, without the possibility of parole, plus ordered to pay about $183 million in restitution.
- Pardoned by POTUS in **Jan 2025**

Oops...

- Ulbricht apparently protected site with CAPTCHA that leaked IP address of Silk Road server
- Operational error, not Tor weakness.
- Remember that **crypto isn’t always the weak link**

And this is how the feds say they located the Silk Road servers:

> "The IP address leak we discovered came from the Silk Road user login interface. Upon examining the individual packets of data being sent back from the website, we noticed that the headers of some of the packets reflected a certain IP address not associated with any known Tor node as the source of the packets. This IP address (the "Subject IP Address") was the only non-Tor source IP address reflected in the traffic we examined."
>
> "The Subject IP Address caught our attention because, if a hidden service is properly configured to work on Tor, the source IP address of traffic sent from the hidden service should appear as the IP address of a Tor node, as opposed to the true IP address of the hidden service, which Tor is designed to conceal. When I typed the Subject IP Address into an ordinary (non-Tor) web browser, a part of the Silk Road login screen (the CAPTCHA prompt) appeared. Based on my training and experience, this indicated that the Subject IP Address was the IP address of the SR Server, and that it was 'leaking' from the SR Server because the computer code underlying the login interface was not properly configured at the time to work on Tor."

http://krebsonsecurity.com/2014/09/dread-pirate-sunk-by-leaky-captcha/

Summary and anonymity trilemma