

Anonymous communication

-

Onion Routing & Tor

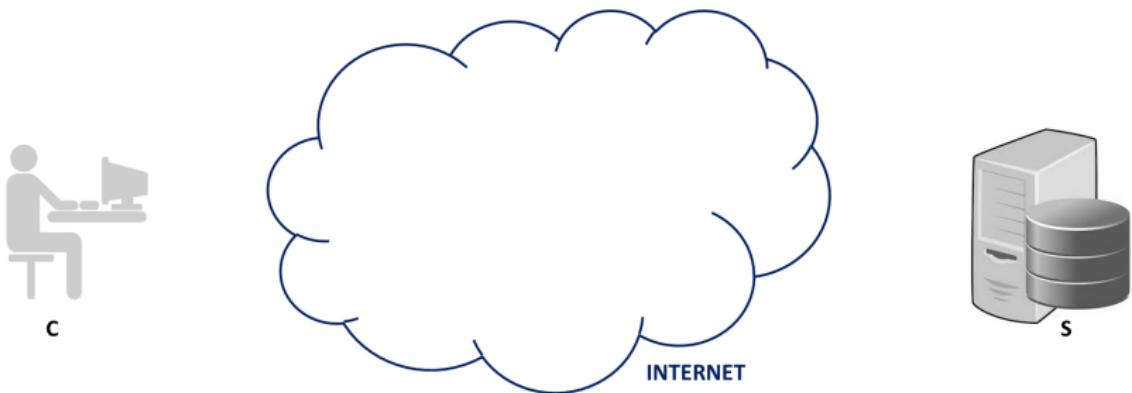
Tariq Elahi¹

School of Informatics
University of Edinburgh

Feb 22, 2021

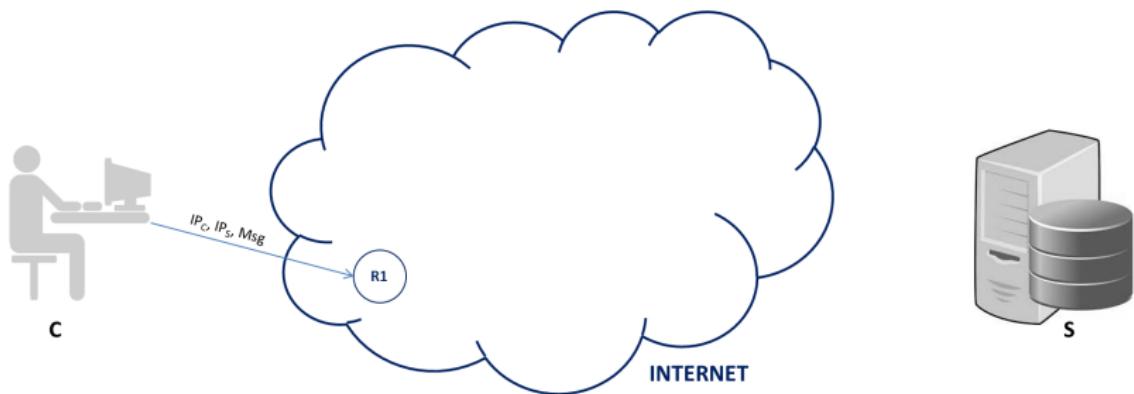
¹with slides developed by Myrto Arapinis

Routing and privacy



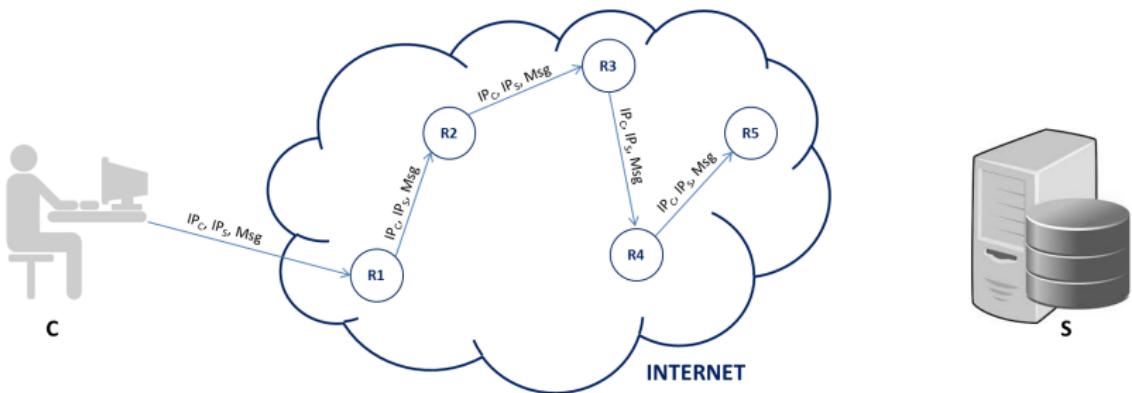
- ▶ Internet routing exposes user's privacy (meta-data like IPs)
- ▶ All routers on the path between source and destination, know the origin and destination of forwarded packets
- ▶ Core internet routers are managed by governments and big corporations (so they can observe a large fraction of Internet activity)

Routing and privacy



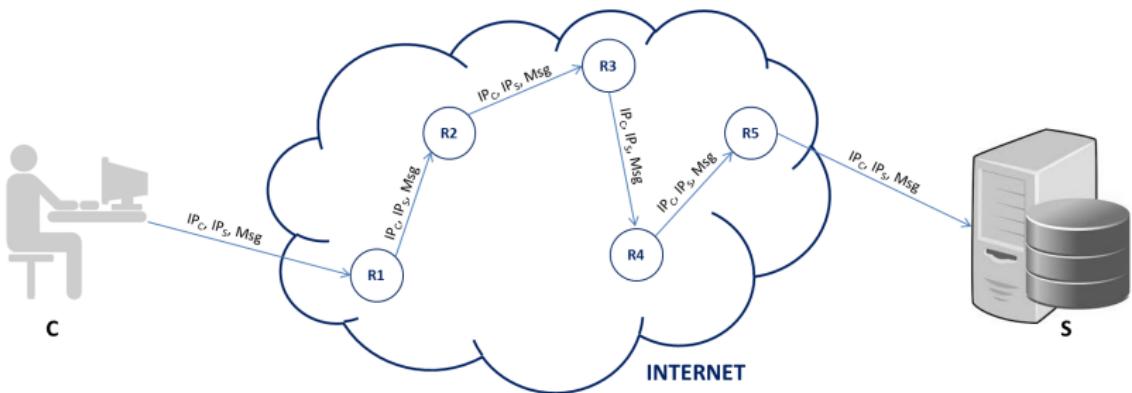
- ▶ Internet routing exposes user's privacy (meta-data like IPs)
- ▶ All routers on the path between source and destination, know the origin and destination of forwarded packets
- ▶ Core internet routers are managed by governments and big corporations (so they can observe a large fraction of Internet activity)

Routing and privacy



- ▶ Internet routing exposes user's privacy (meta-data like IPs)
- ▶ All routers on the path between source and destination, know the origin and destination of forwarded packets
- ▶ Core internet routers are managed by governments and big corporations (so they can observe a large fraction of Internet activity)

Routing and privacy



- ▶ Internet routing exposes user's privacy (meta-data like IPs)
- ▶ All routers on the path between source and destination, know the origin and destination of forwarded packets
- ▶ Core internet routers are managed by governments and big corporations (so they can observe a large fraction of Internet activity)

Today's lecture



Stand up for privacy and freedom online

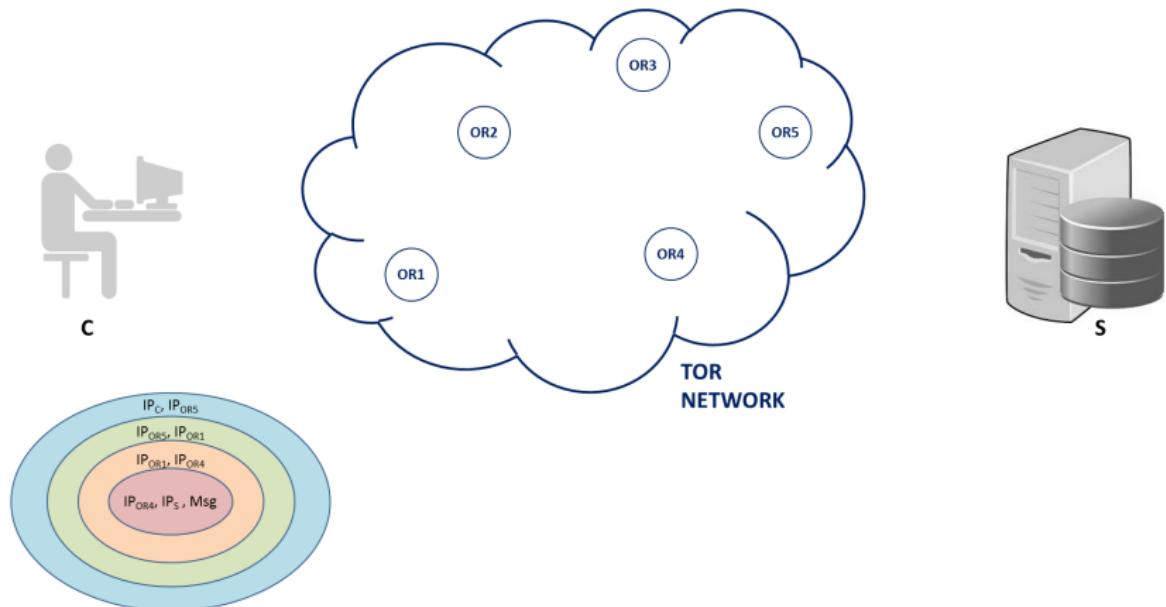
[R. Dingledine, N. Mathewson, and P. F. Syverson: "Tor: The Second-Generation Onion Router", USENIX Security Symposium 2004]

Idea: combine advantages of mixes and proxies

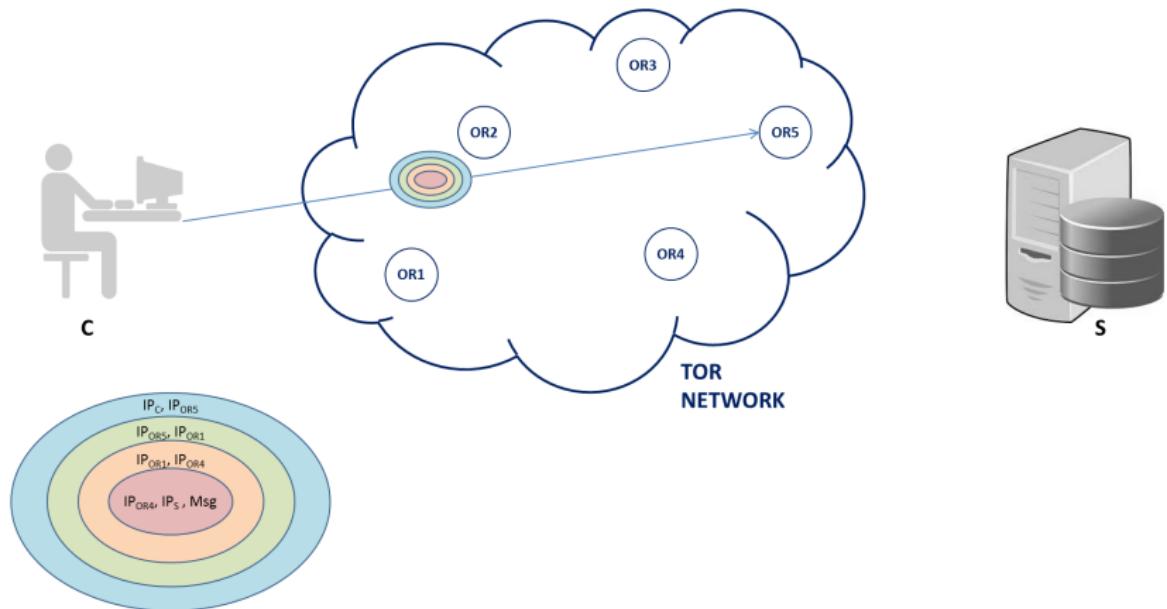
- ▶ use public-key crypto only to establish circuit
- ▶ use symmetric-key crypto to exchange data
- ▶ distribute trust like mixes
- ▶ do not delay or batch like mixes (low-latency)

But does not defend against adversary that observes the whole network

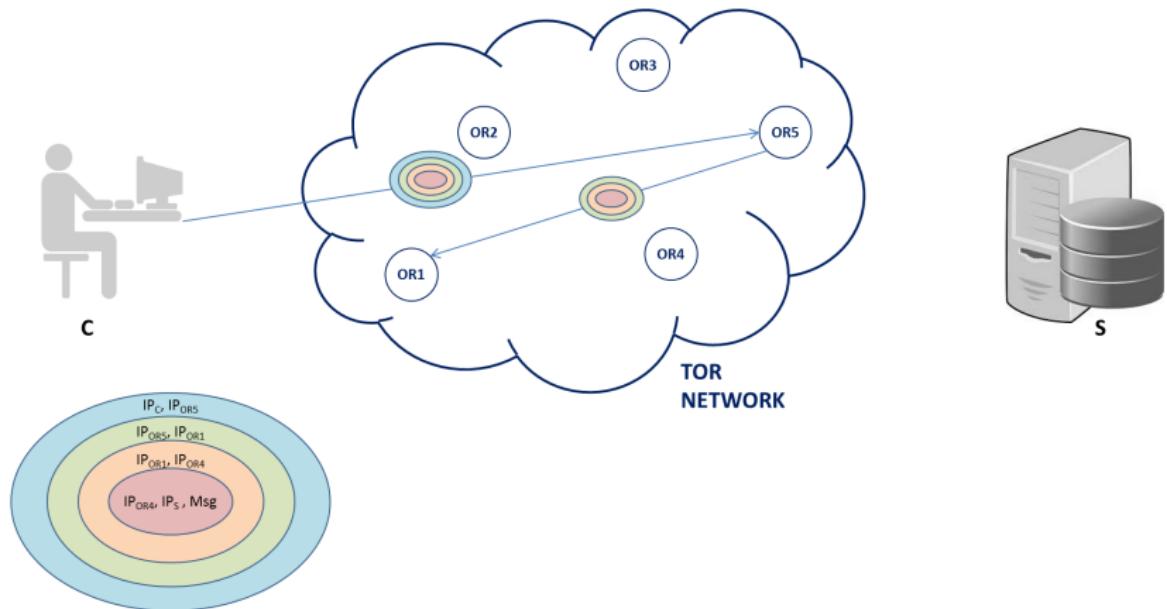
Tor's main ingredient: the onion



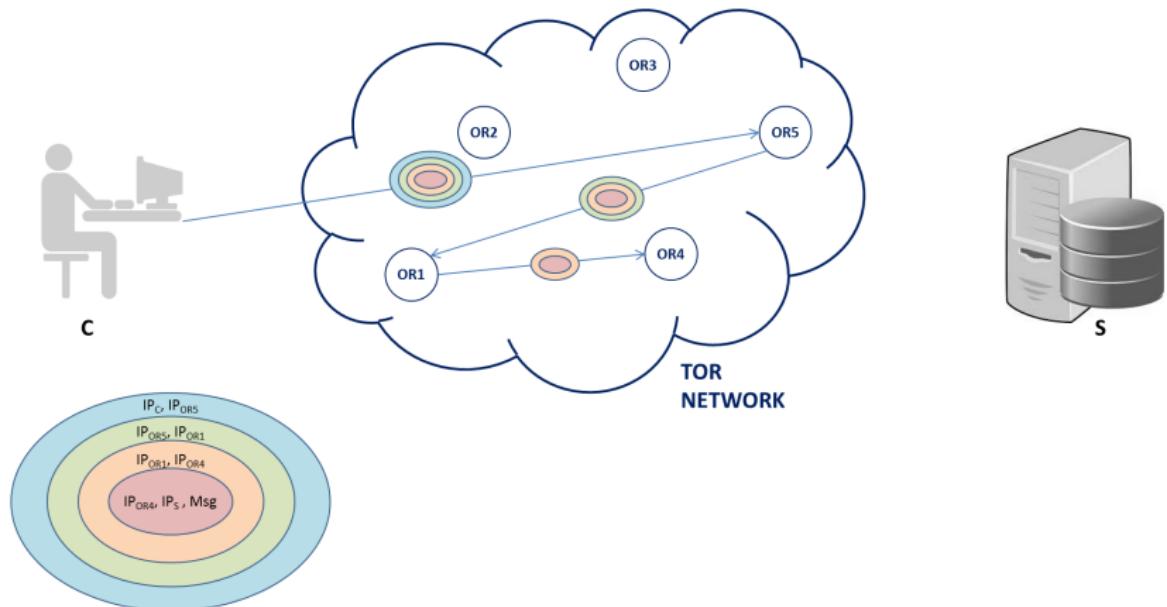
Tor's main ingredient: the onion



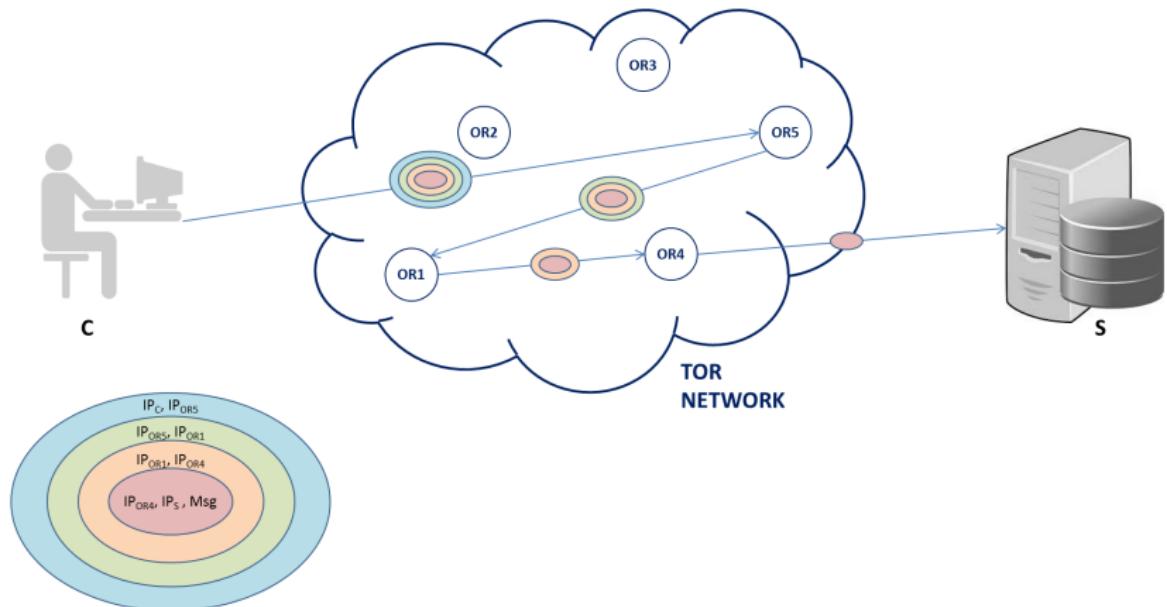
Tor's main ingredient: the onion



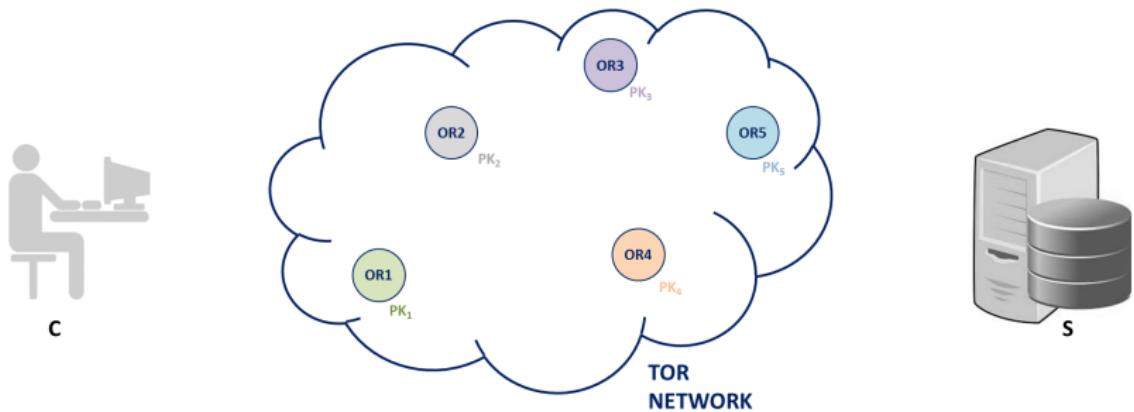
Tor's main ingredient: the onion



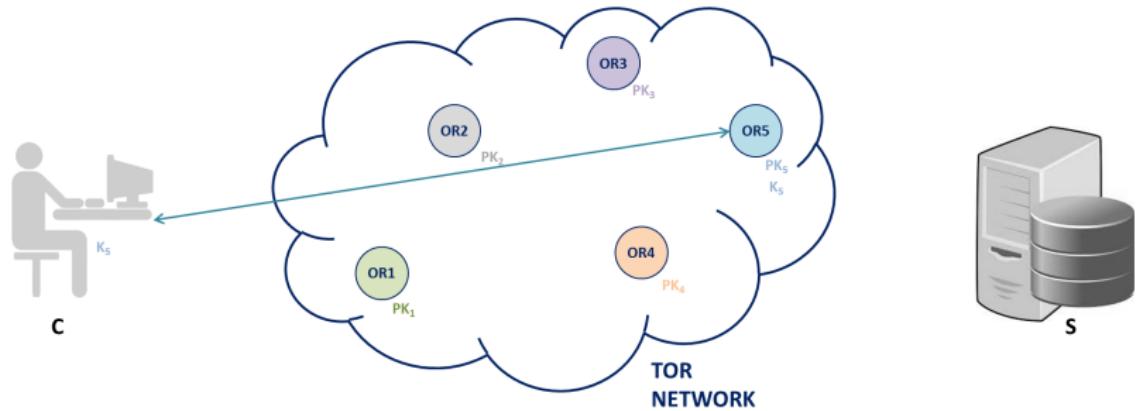
Tor's main ingredient: the onion



Tor circuit setup

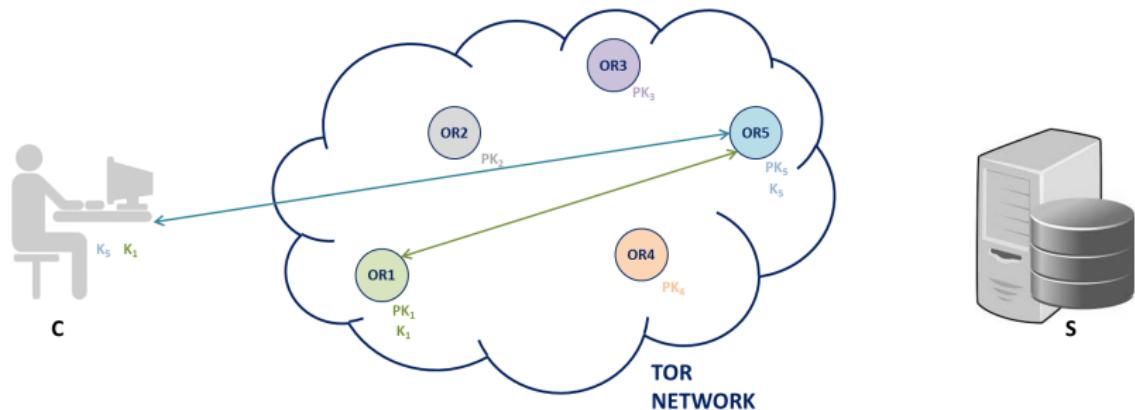


Tor circuit setup



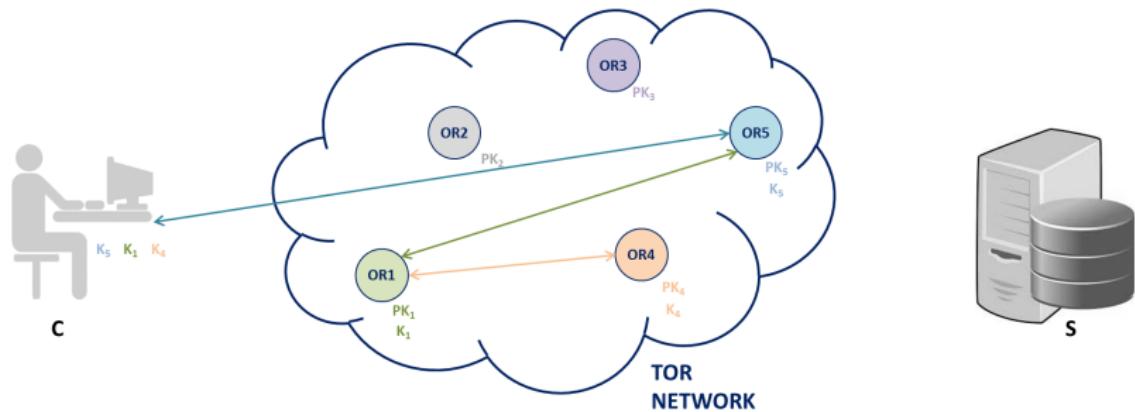
- ▶ C establishes session key K_5 and circuit with Onion Router OR_5

Tor circuit setup



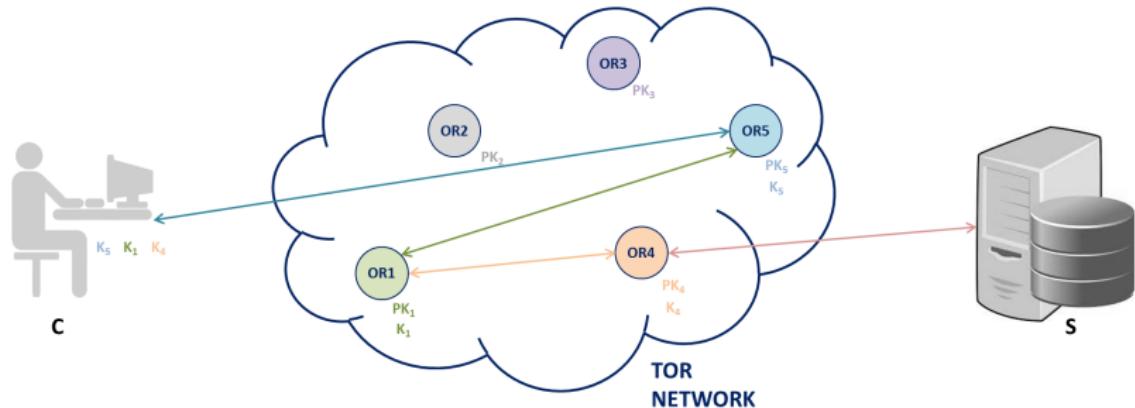
- ▶ C establishes session key K_5 and circuit with Onion Router OR_5
- ▶ C tunnels through that circuit to extend to Onion Router OR_1

Tor circuit setup



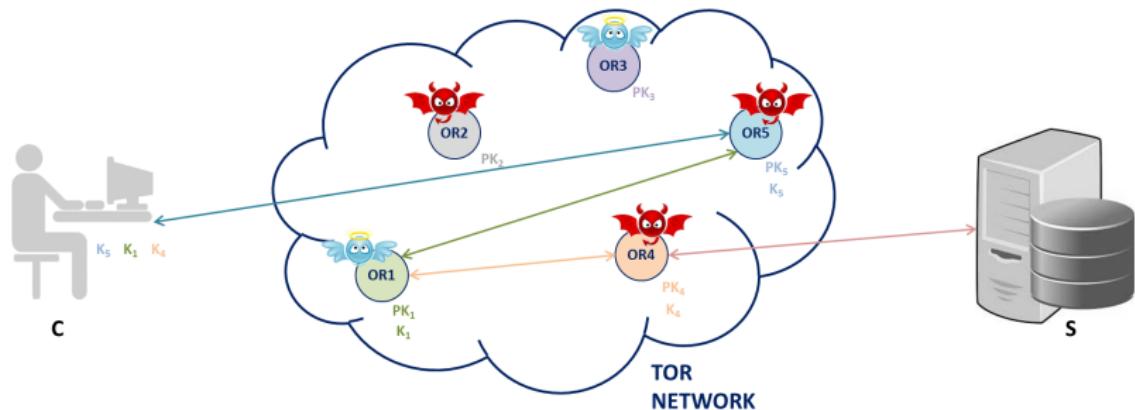
- ▶ C establishes session key K_5 and circuit with Onion Router OR_5
- ▶ C tunnels through that circuit to extend to Onion Router OR_1
- ▶ C tunnels through that extended circuit to extend to Onion Router OR_4

Tor circuit setup



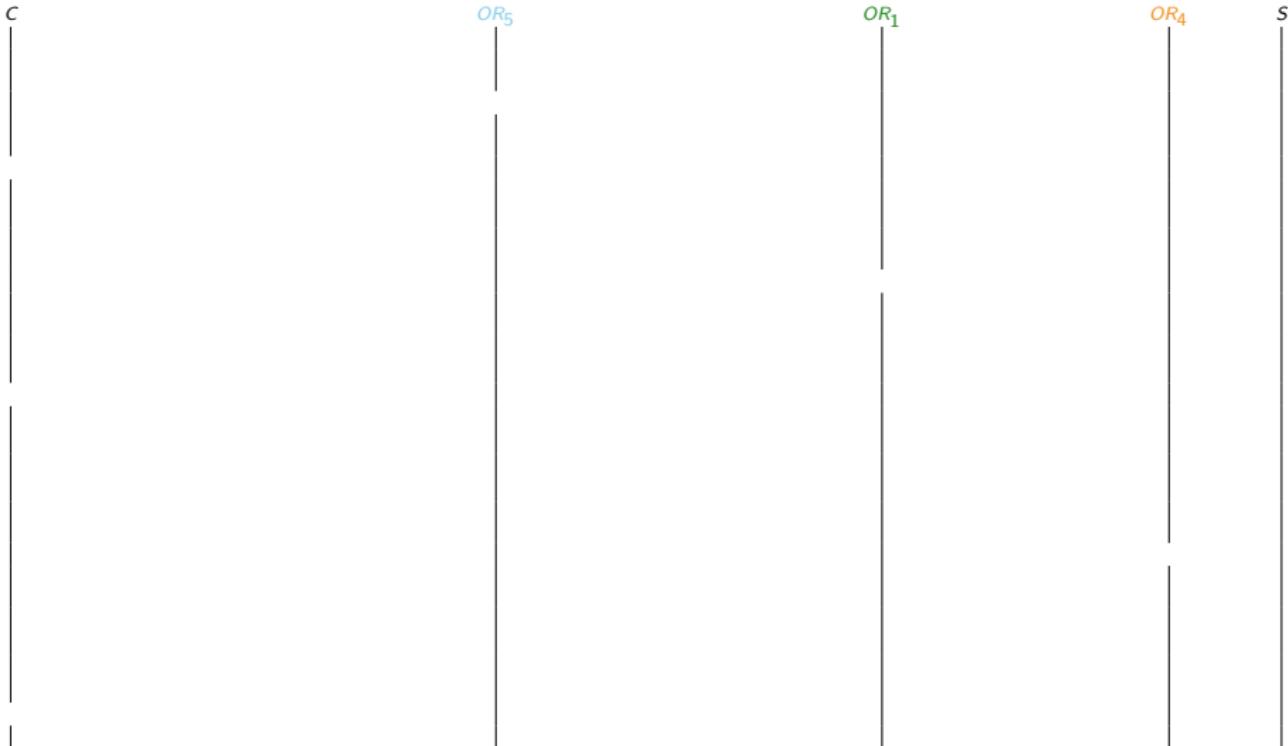
- ▶ C establishes session key K_5 and circuit with Onion Router OR_5
- ▶ C tunnels through that circuit to extend to Onion Router OR_1
- ▶ C tunnels through that extended circuit to extend to Onion Router OR_4
- ▶ Client applications connect and communicate over established Tor circuit

Tor circuit setup

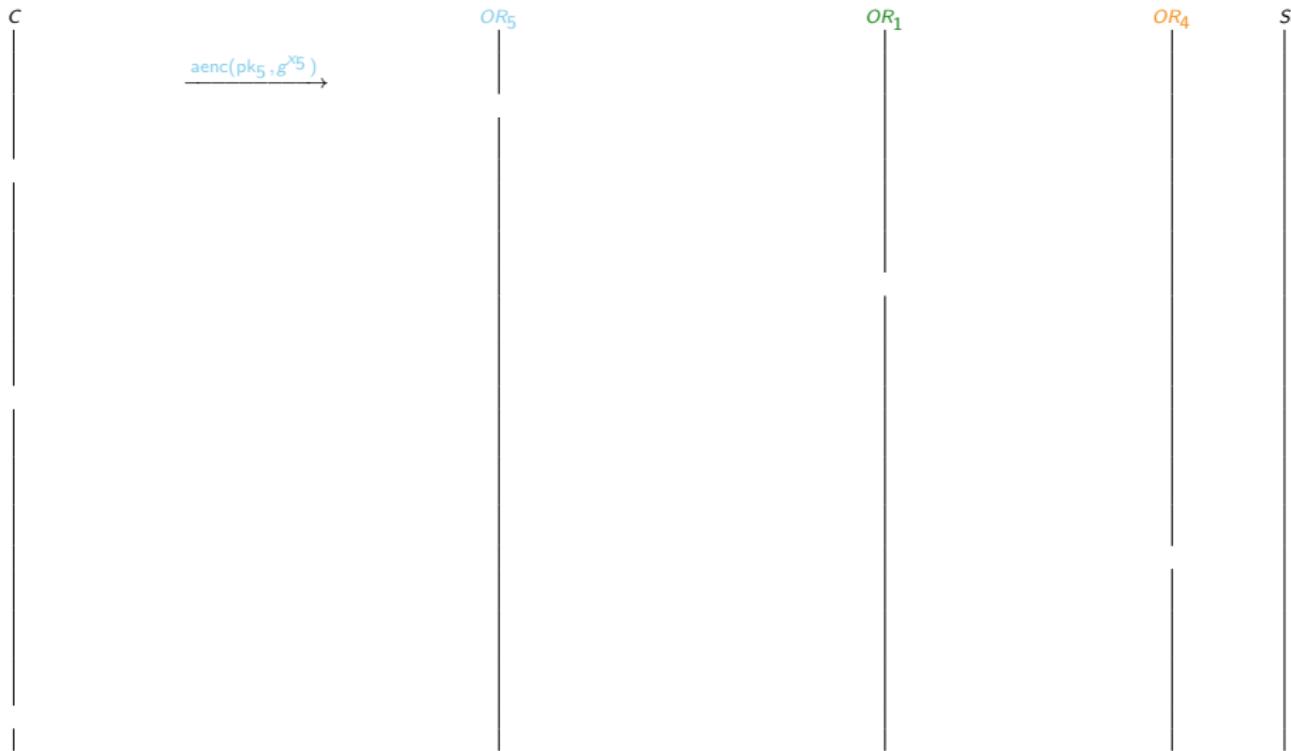


- ▶ C establishes session key K_5 and circuit with Onion Router OR_5
- ▶ C tunnels through that circuit to extend to Onion Router OR_1
- ▶ C tunnels through that extended circuit to extend to Onion Router OR_4
- ▶ Client applications connect and communicate over established Tor circuit
- ▶ A single honest Onion Router on the Tor circuit guarantees anonymity against an attacker controlling some Onion Routers

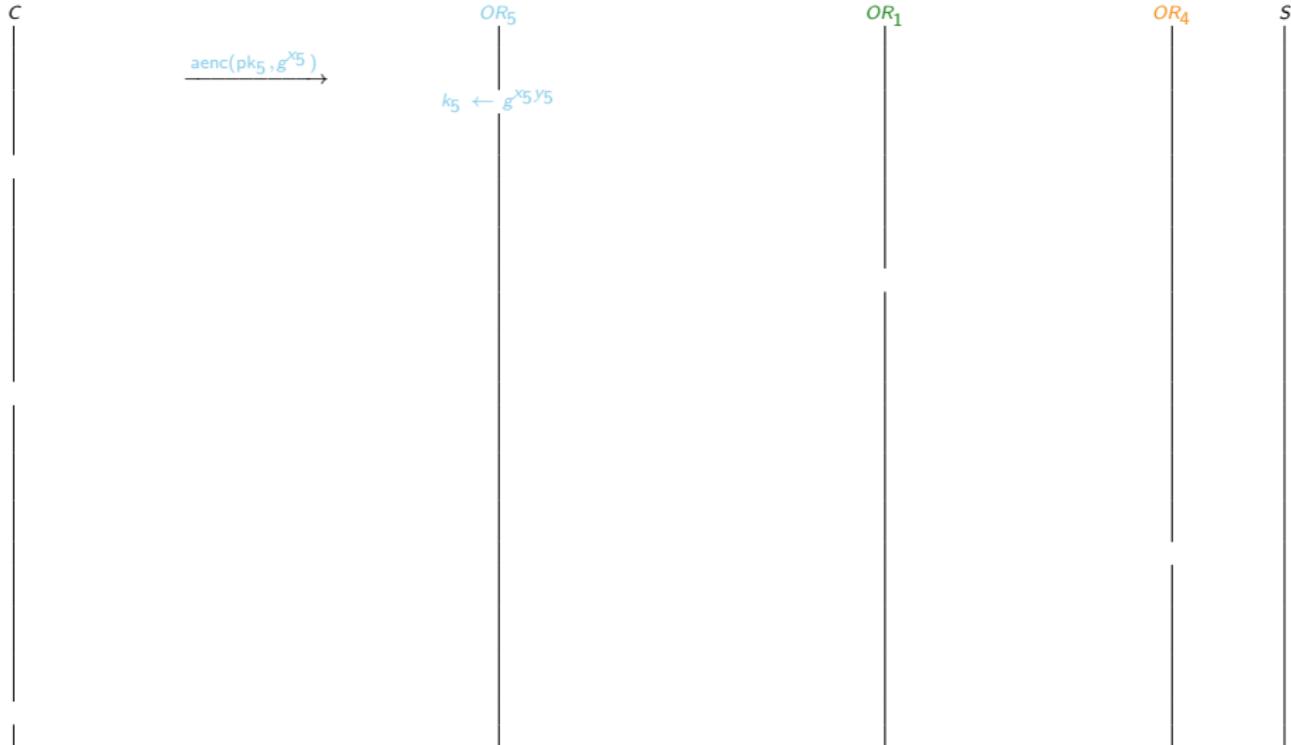
The (simplified) Tor message flow - circuit setup



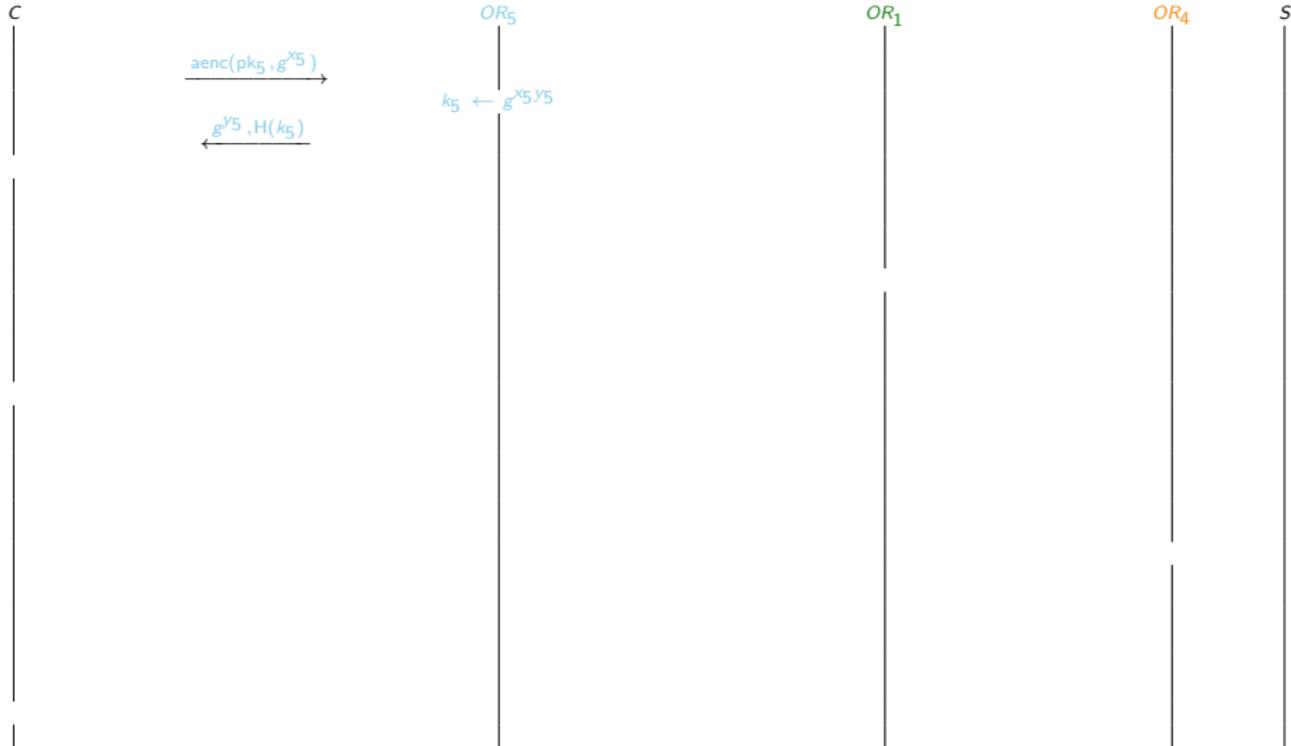
The (simplified) Tor message flow - circuit setup



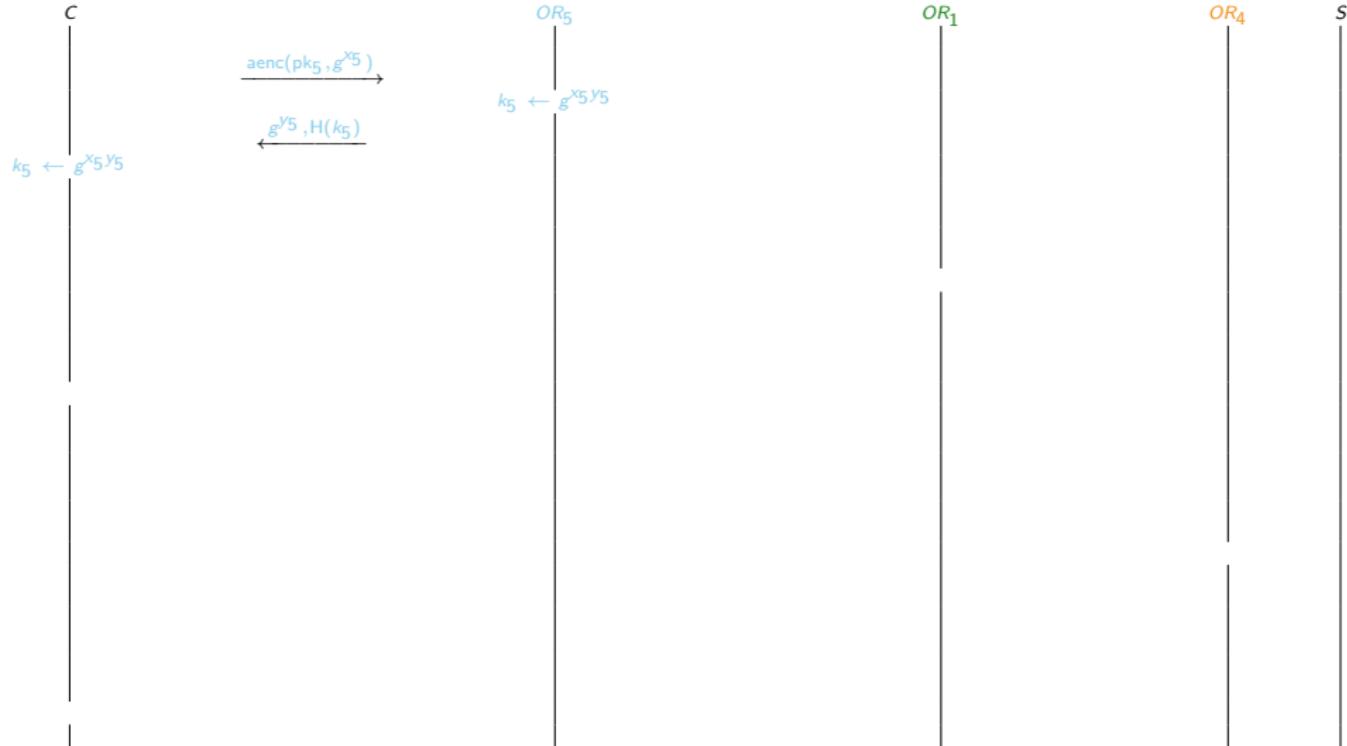
The (simplified) Tor message flow - circuit setup



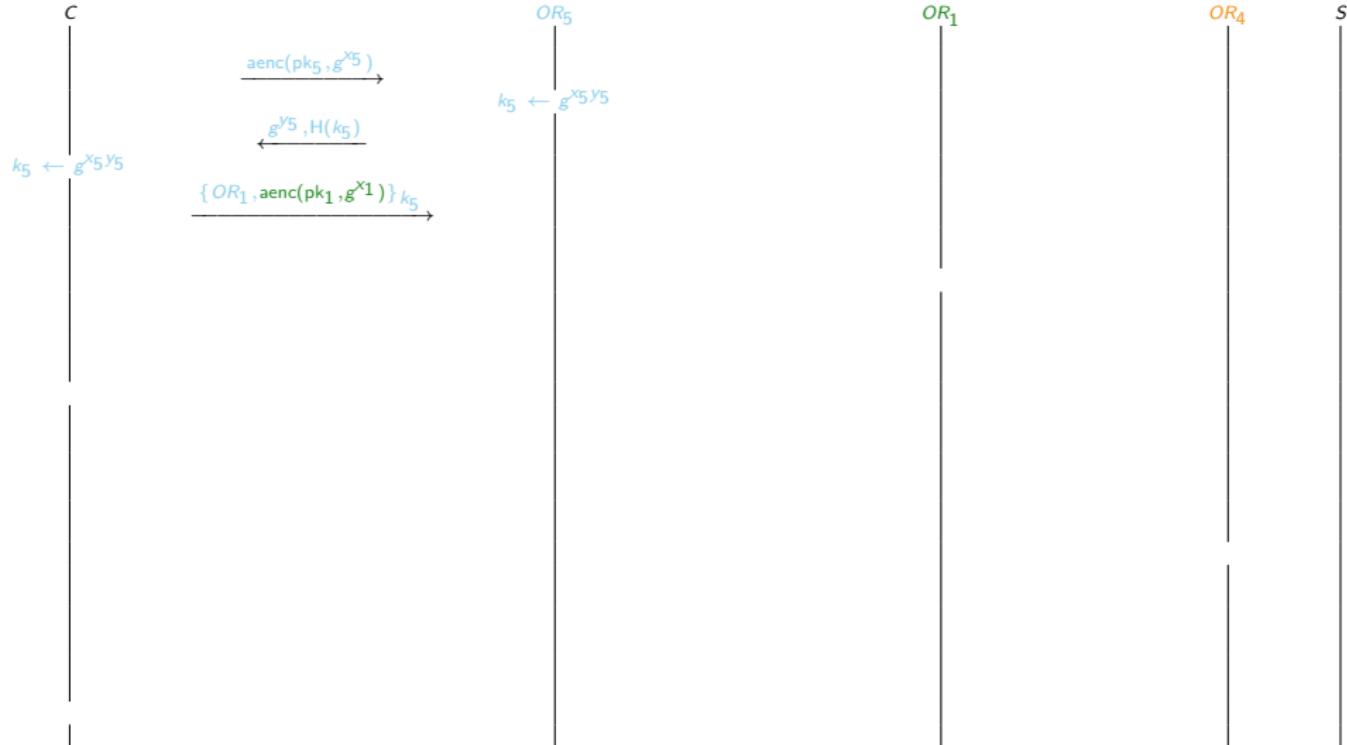
The (simplified) Tor message flow - circuit setup



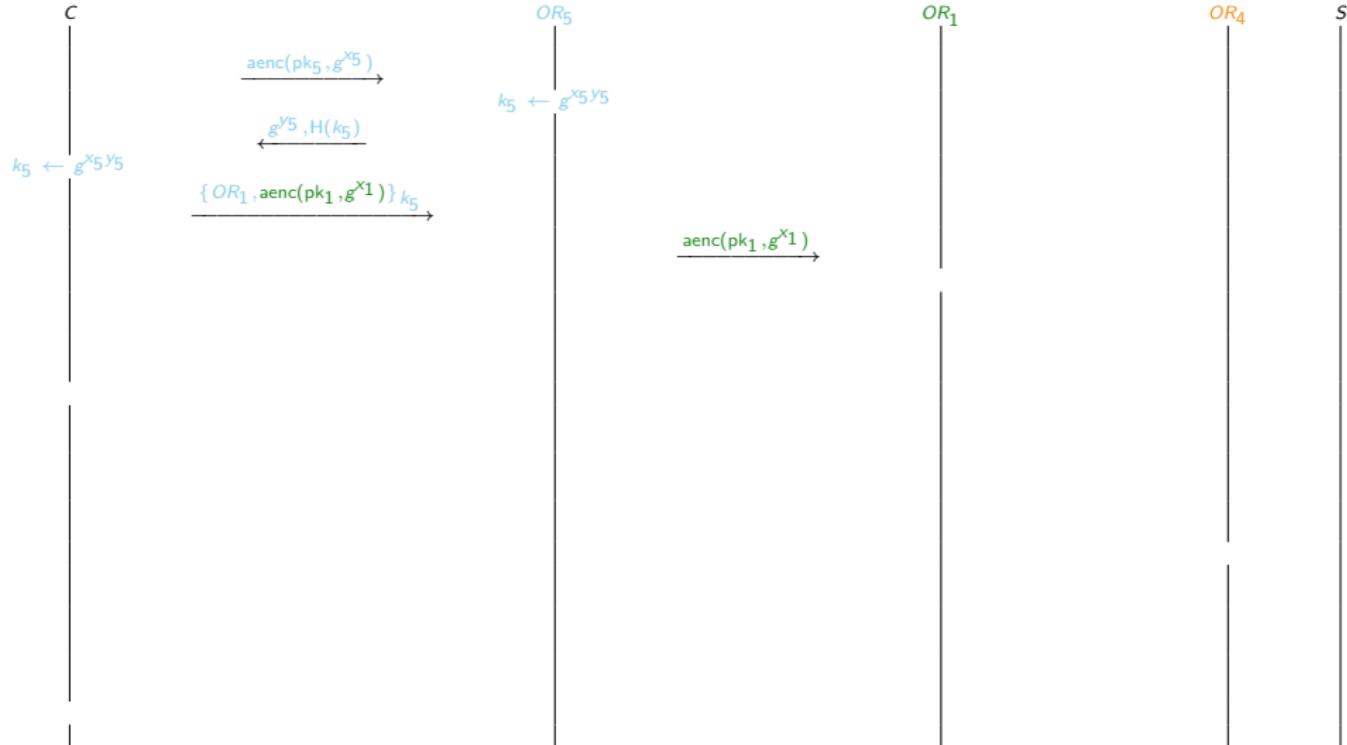
The (simplified) Tor message flow - circuit setup



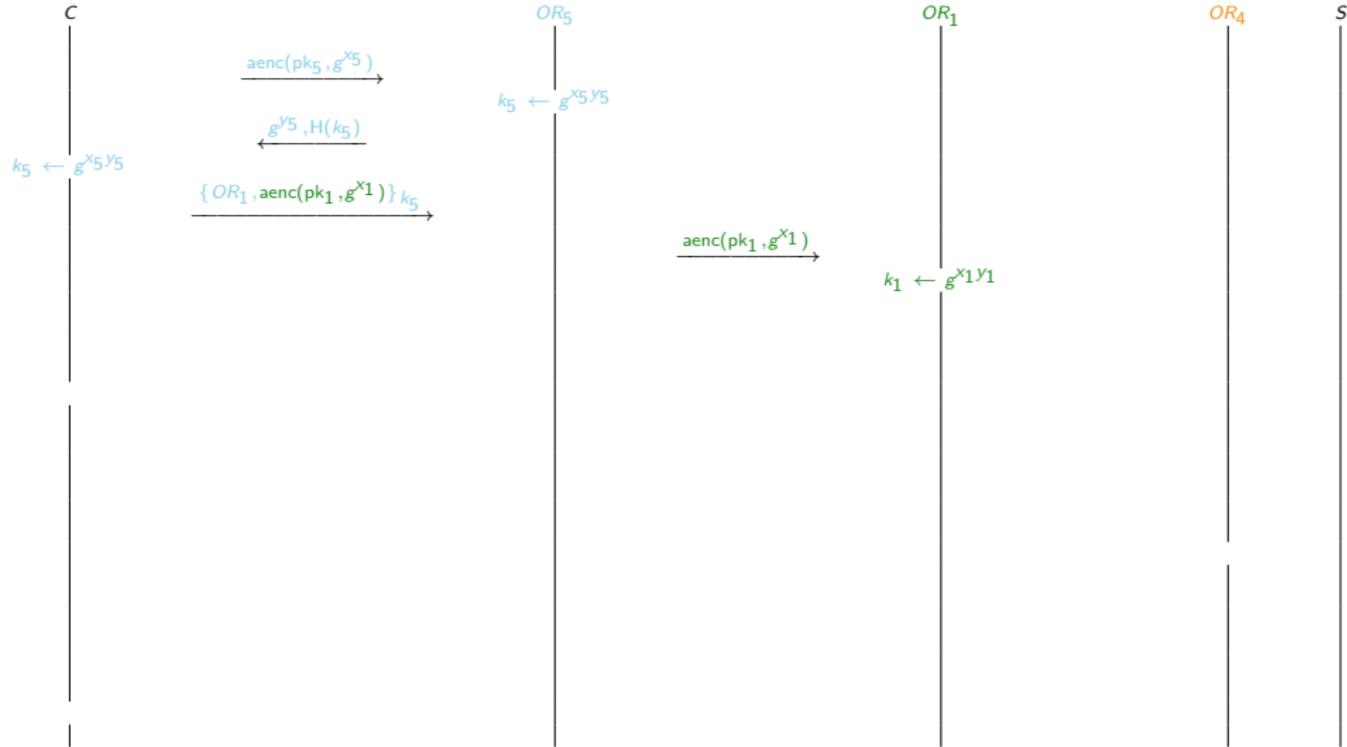
The (simplified) Tor message flow - circuit setup



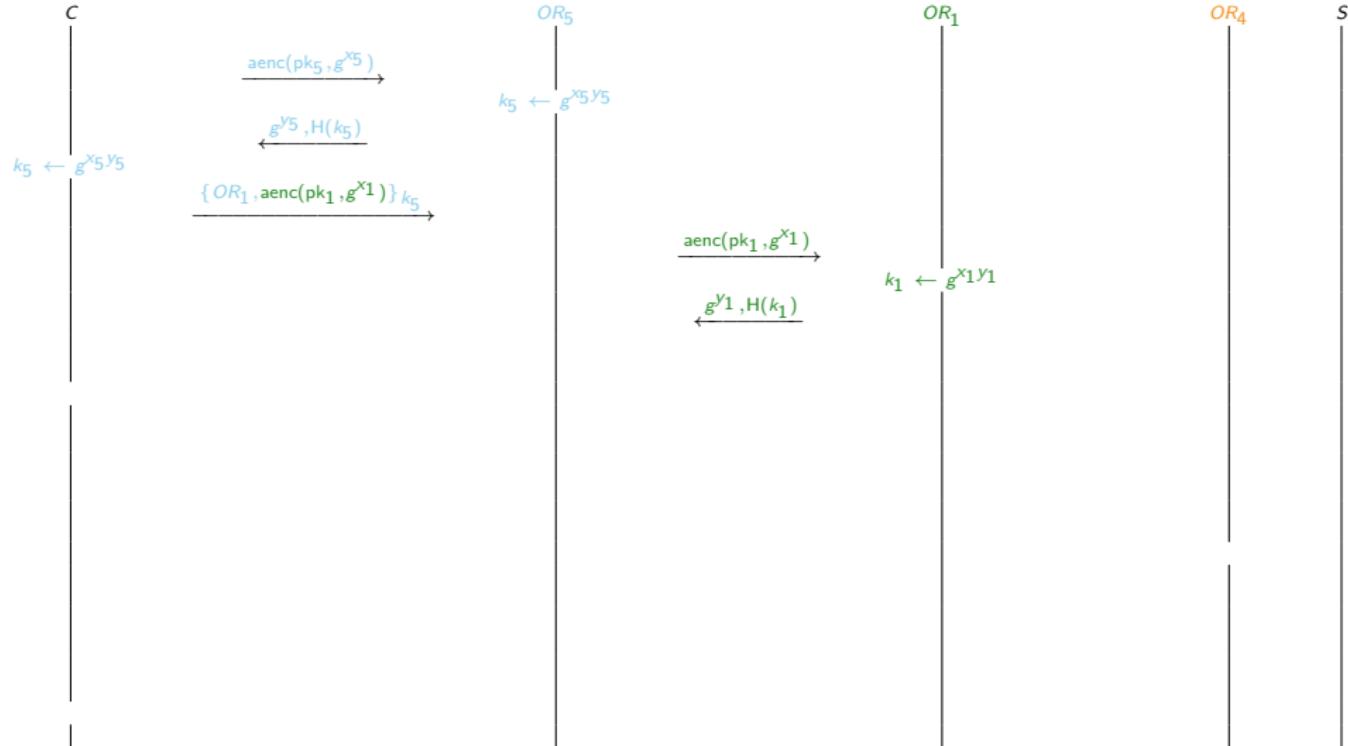
The (simplified) Tor message flow - circuit setup



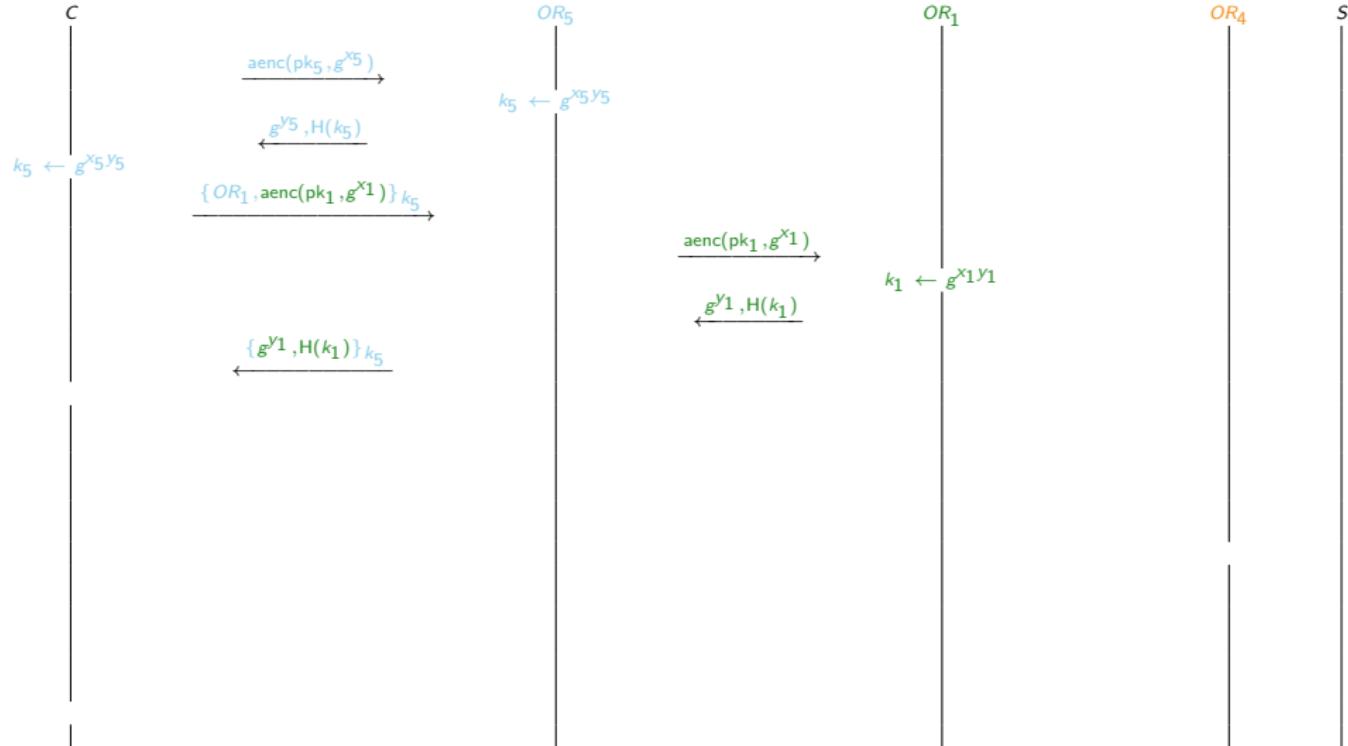
The (simplified) Tor message flow - circuit setup



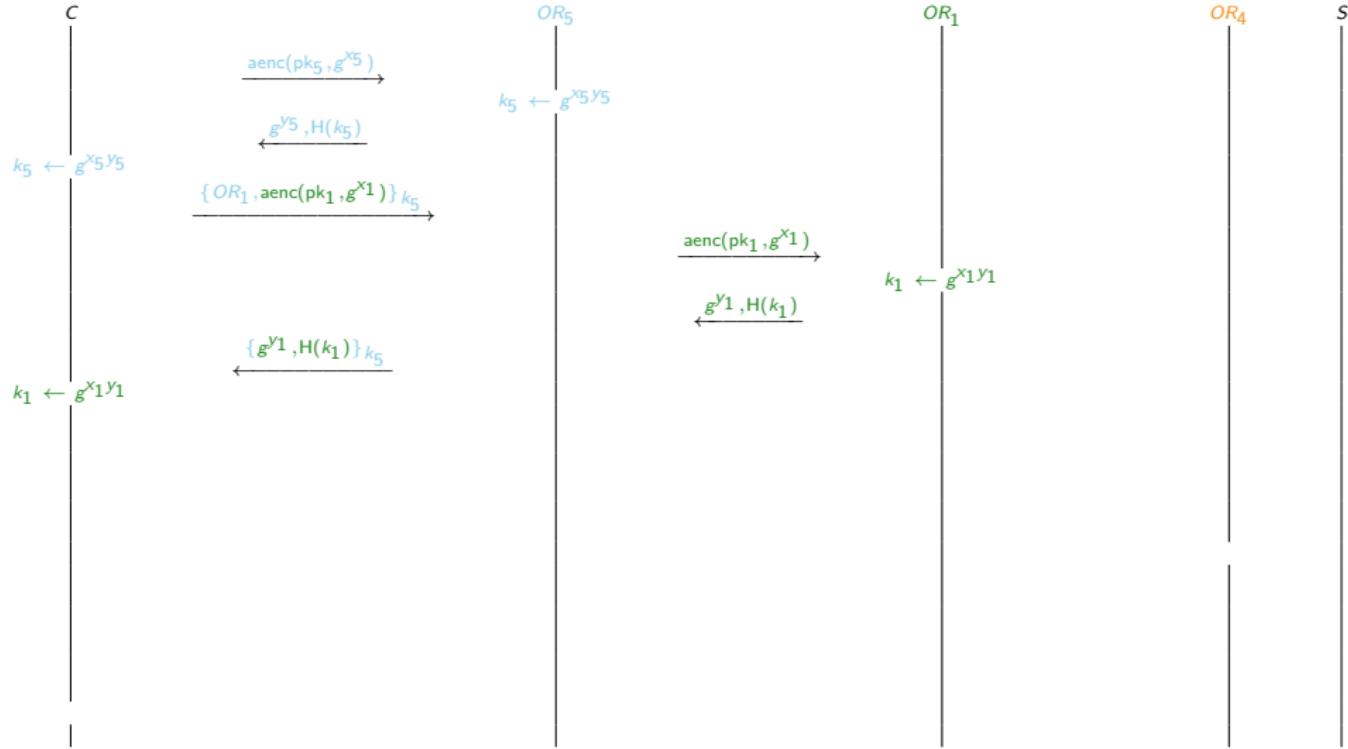
The (simplified) Tor message flow - circuit setup



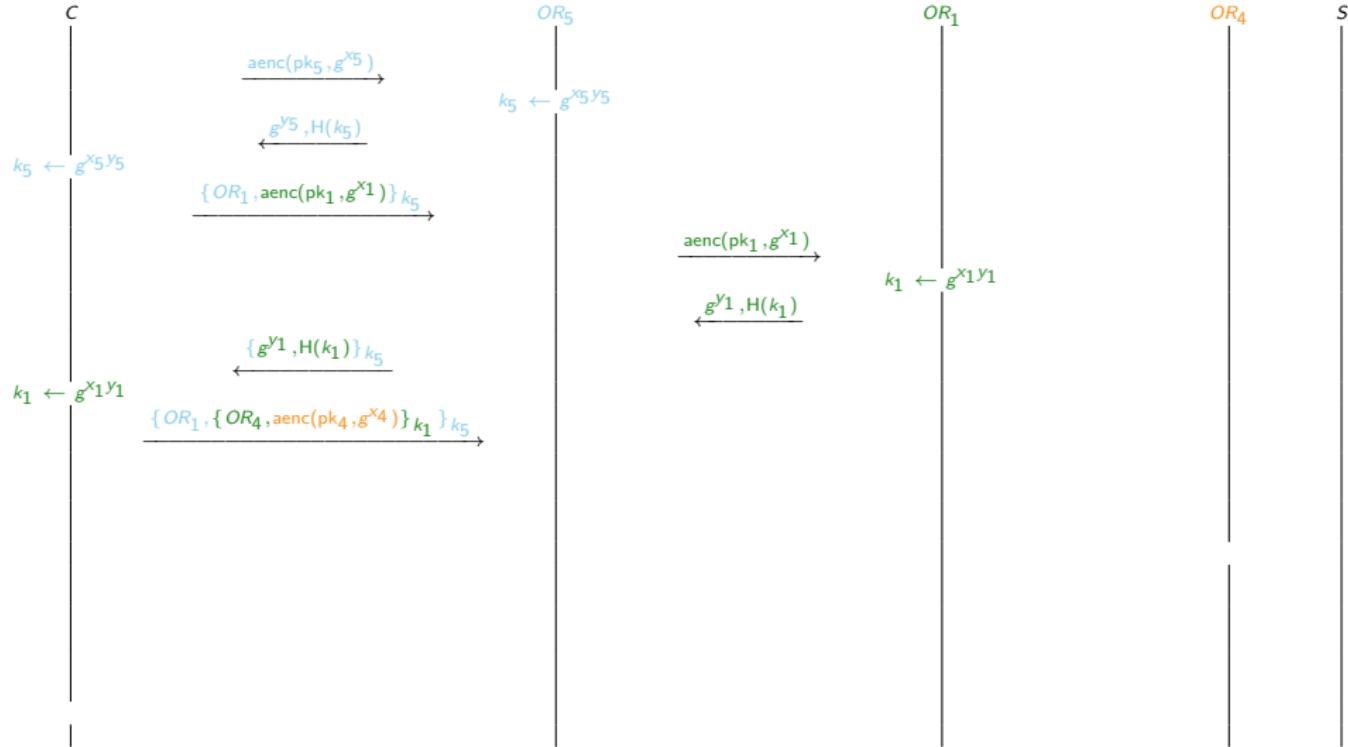
The (simplified) Tor message flow - circuit setup



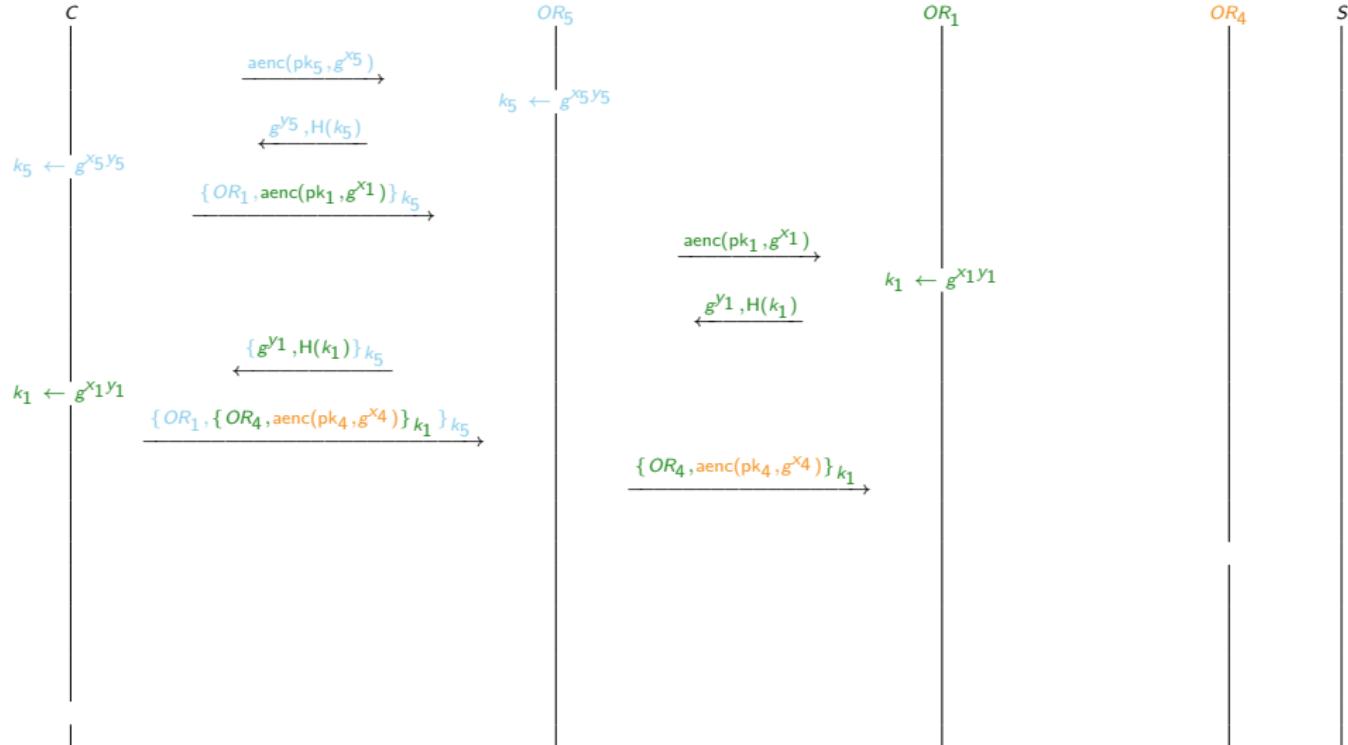
The (simplified) Tor message flow - circuit setup



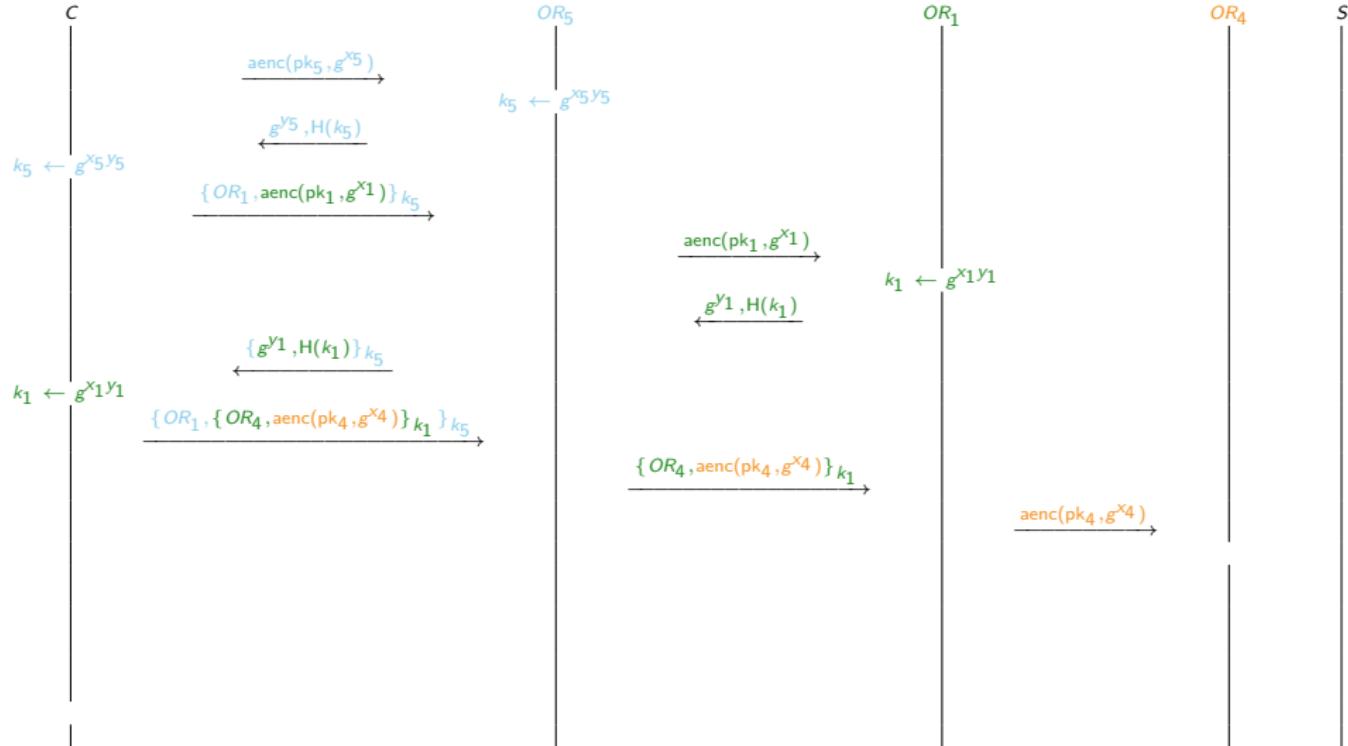
The (simplified) Tor message flow - circuit setup



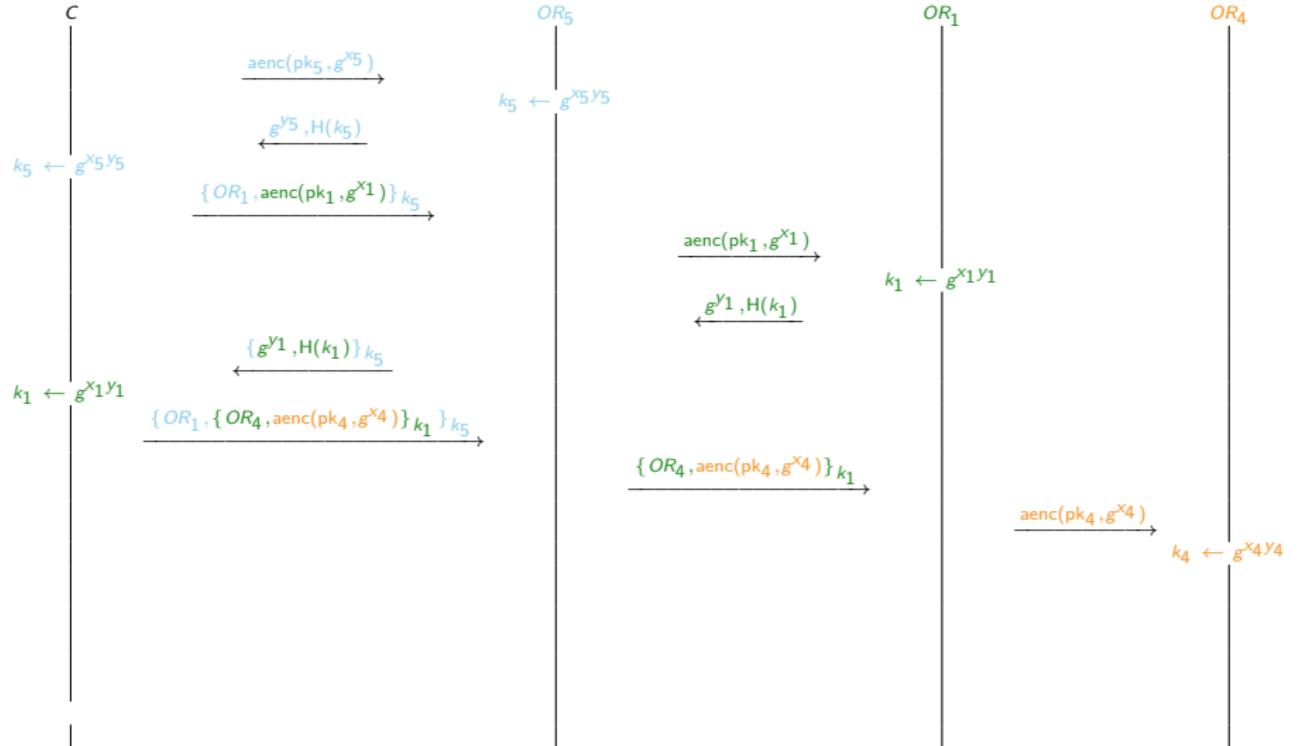
The (simplified) Tor message flow - circuit setup



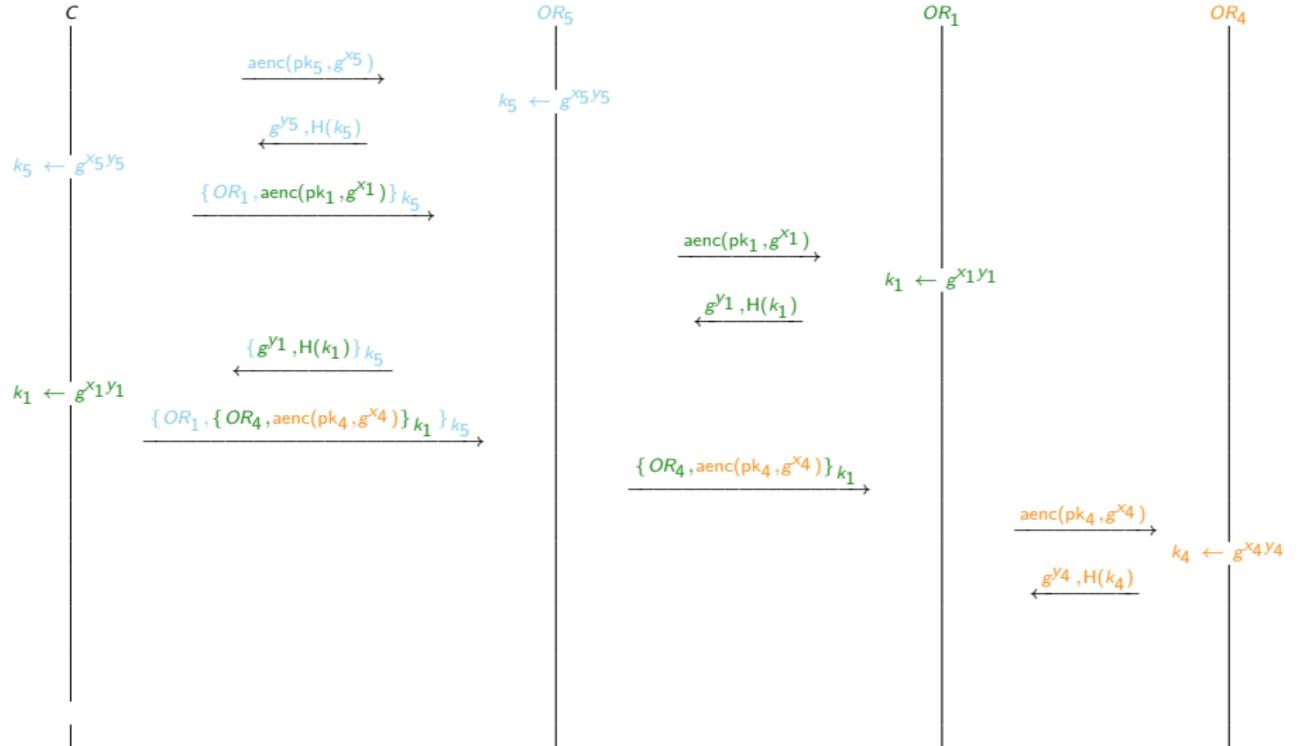
The (simplified) Tor message flow - circuit setup



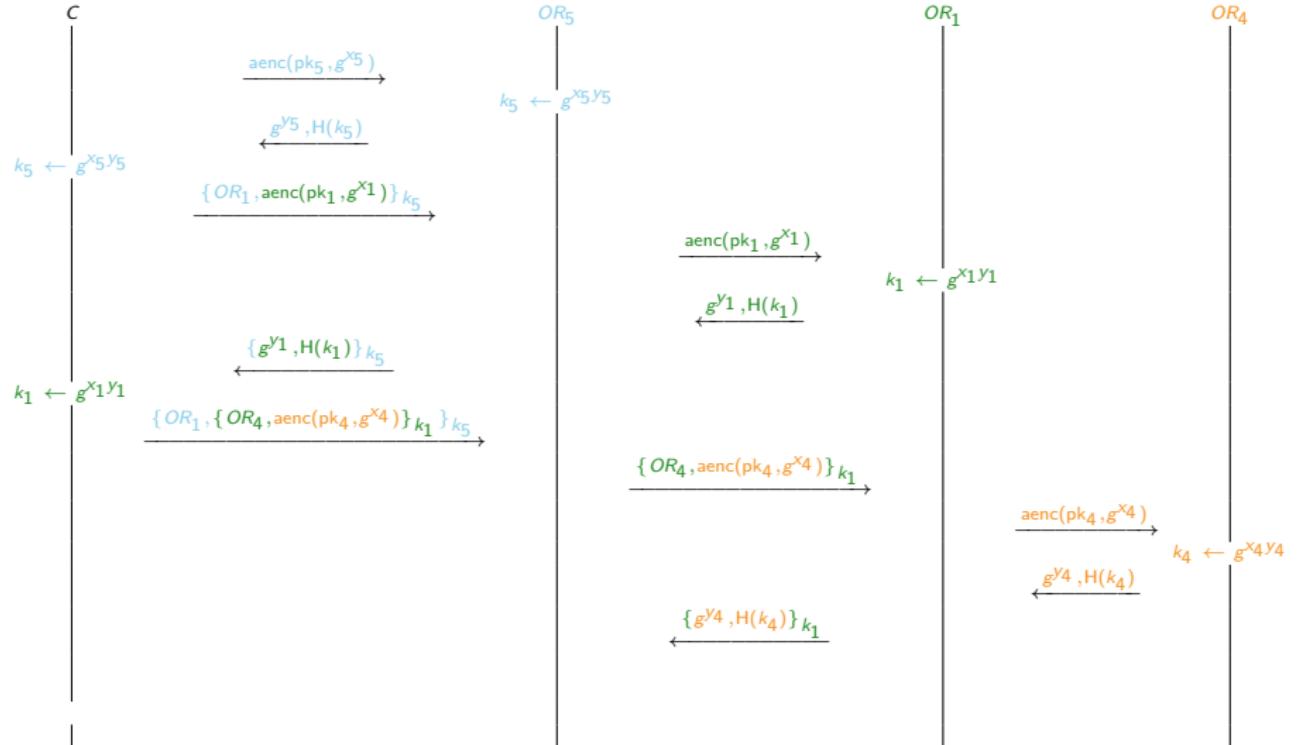
The (simplified) Tor message flow - circuit setup



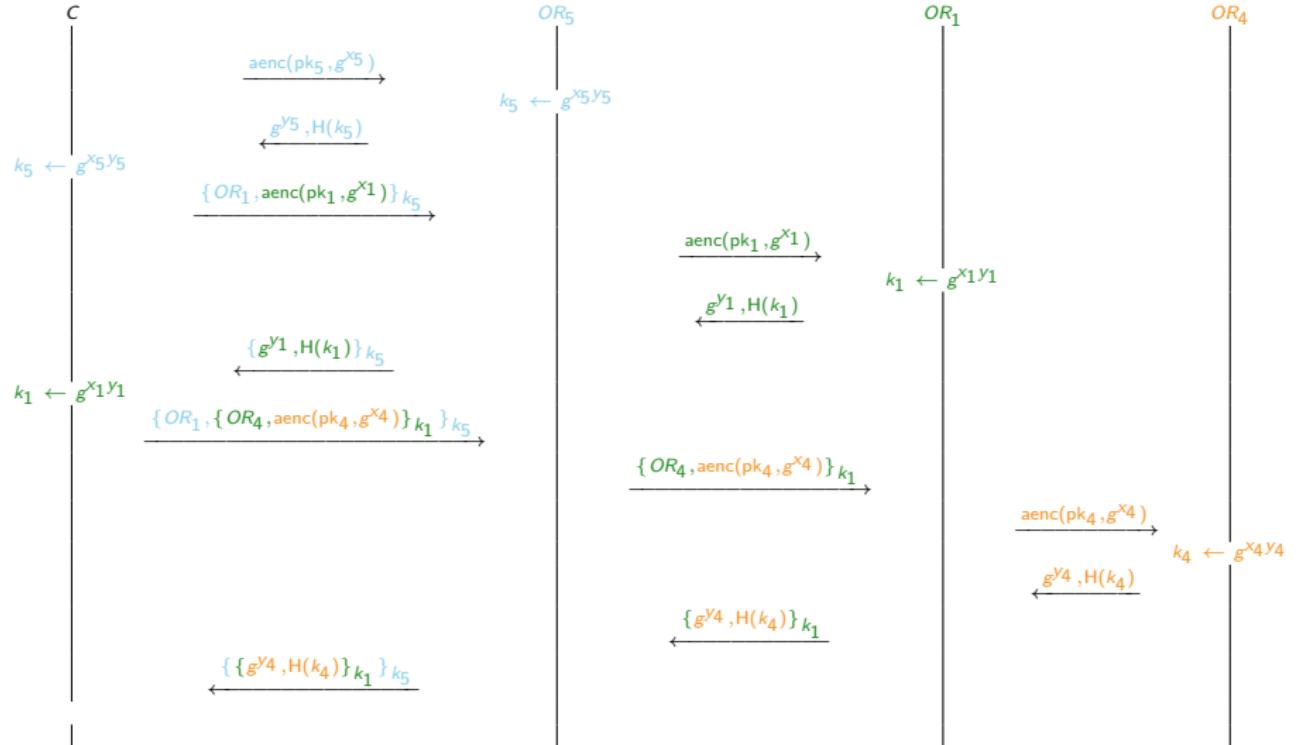
The (simplified) Tor message flow - circuit setup



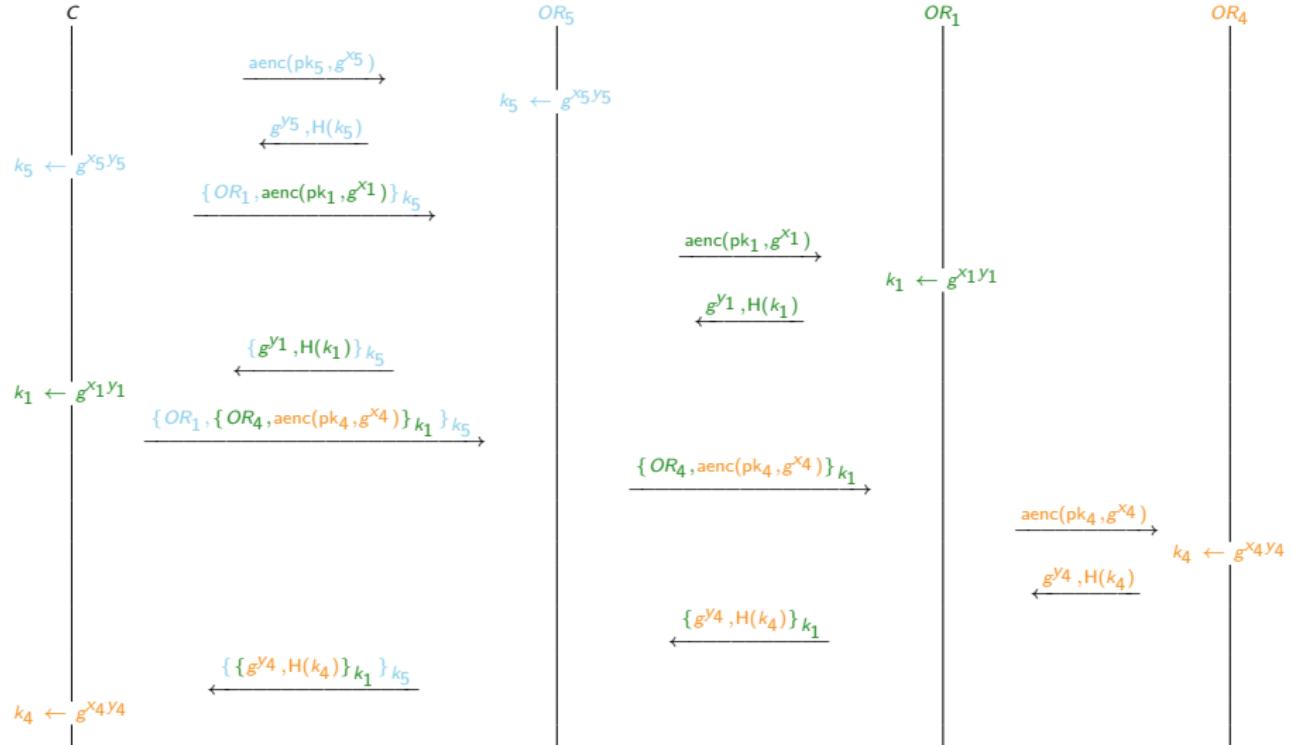
The (simplified) Tor message flow - circuit setup



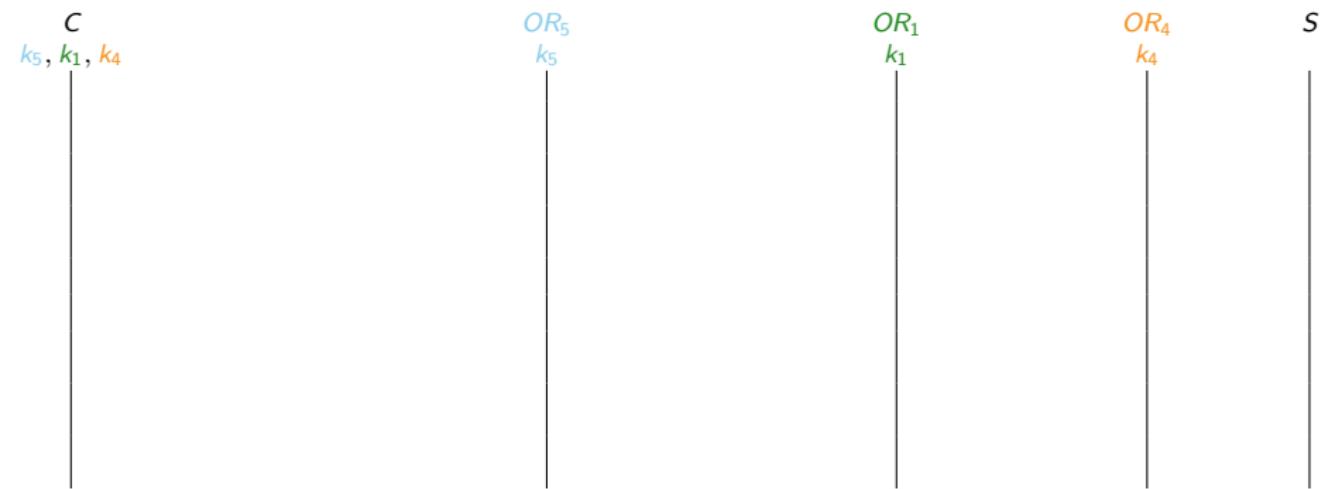
The (simplified) Tor message flow - circuit setup



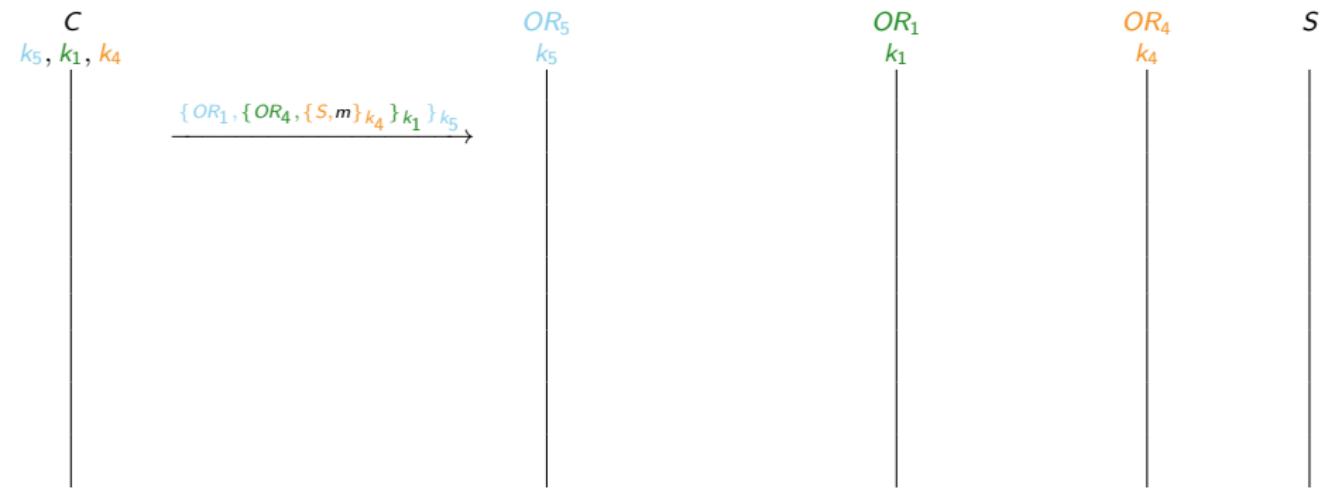
The (simplified) Tor message flow - circuit setup



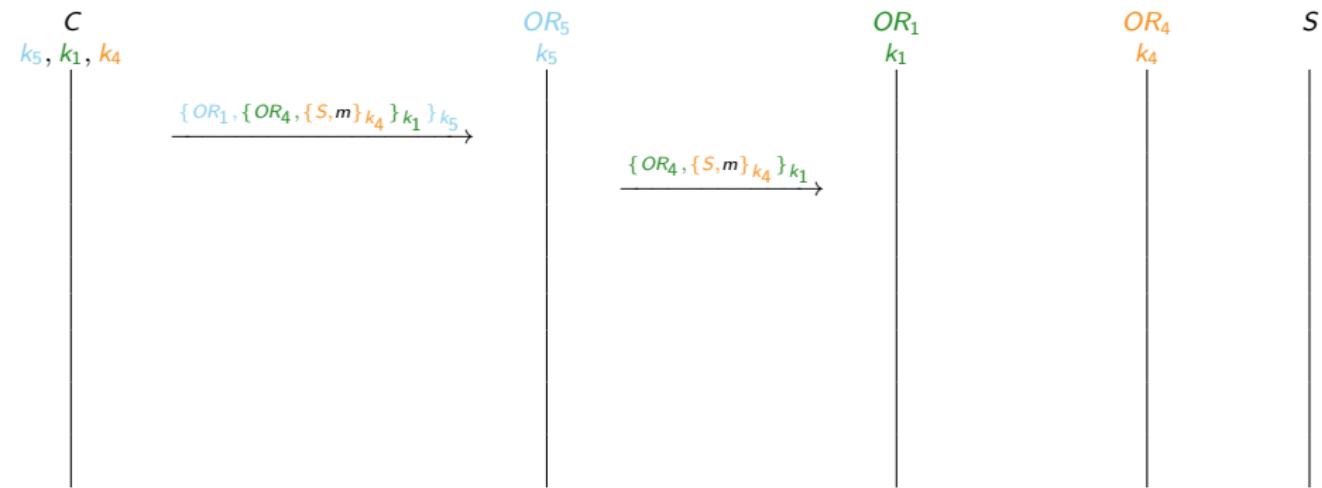
The (simplified) Tor message flow - actual communication



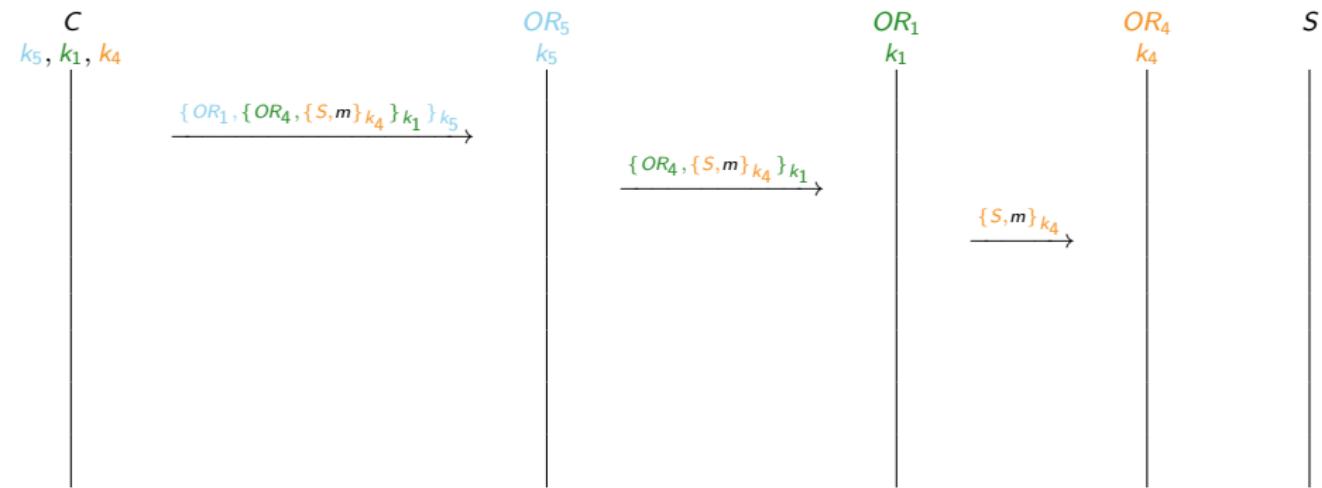
The (simplified) Tor message flow - actual communication



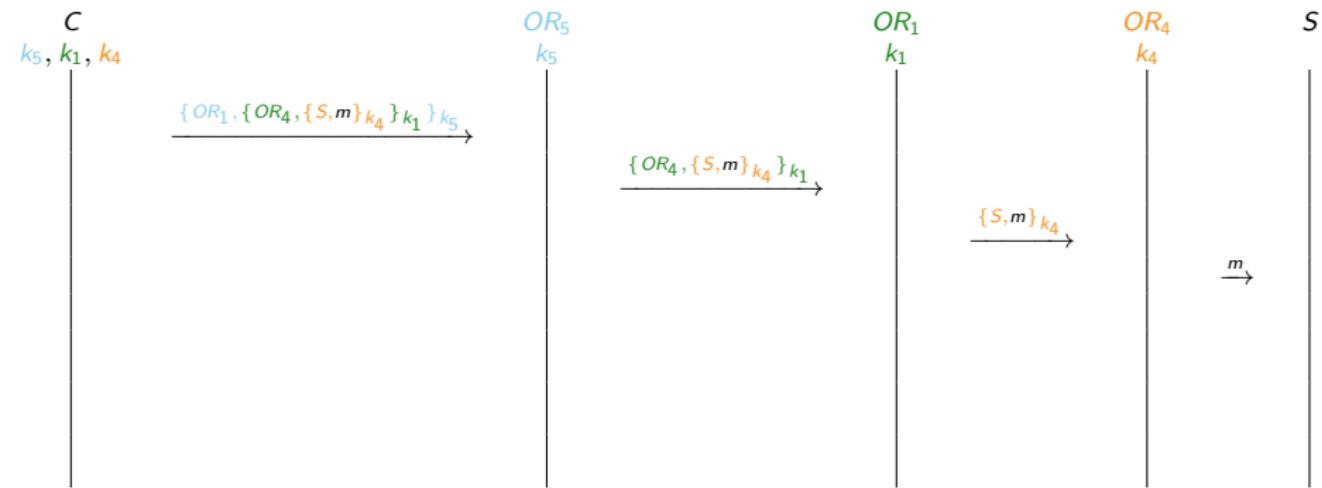
The (simplified) Tor message flow - actual communication



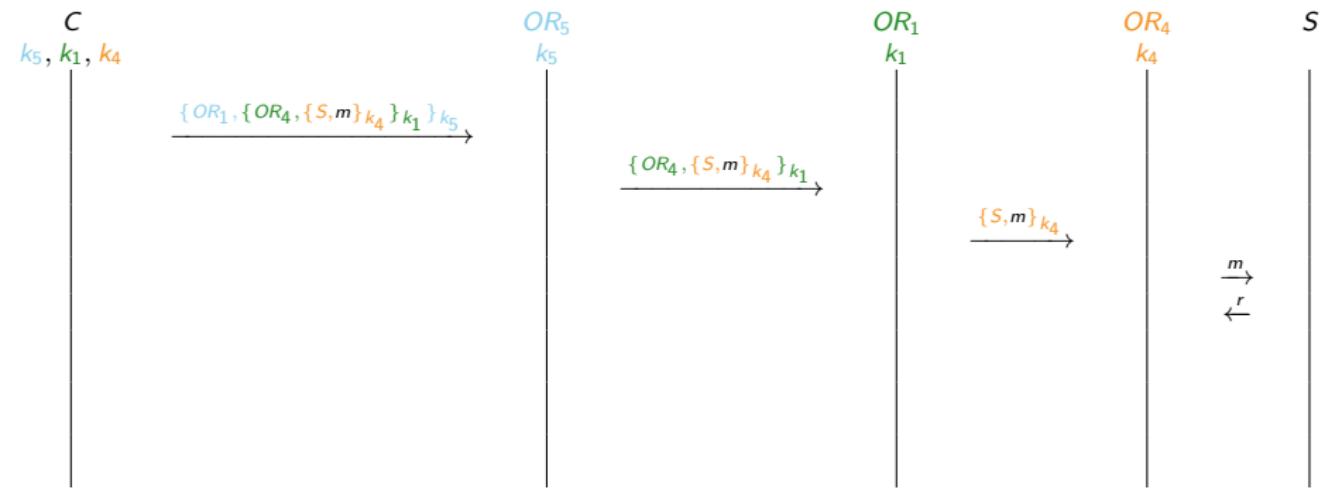
The (simplified) Tor message flow - actual communication



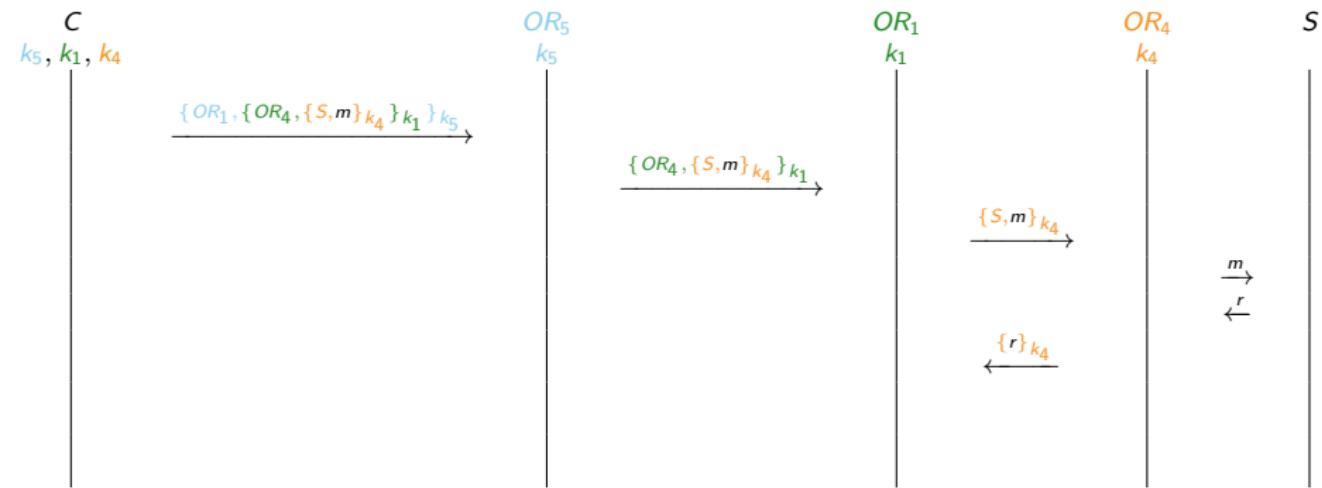
The (simplified) Tor message flow - actual communication



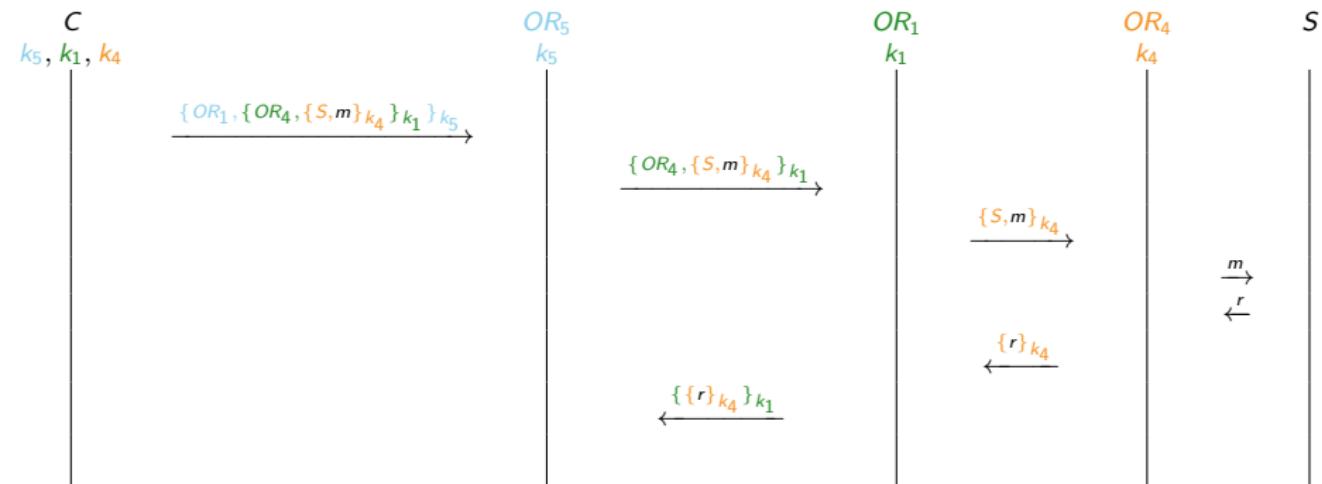
The (simplified) Tor message flow - actual communication



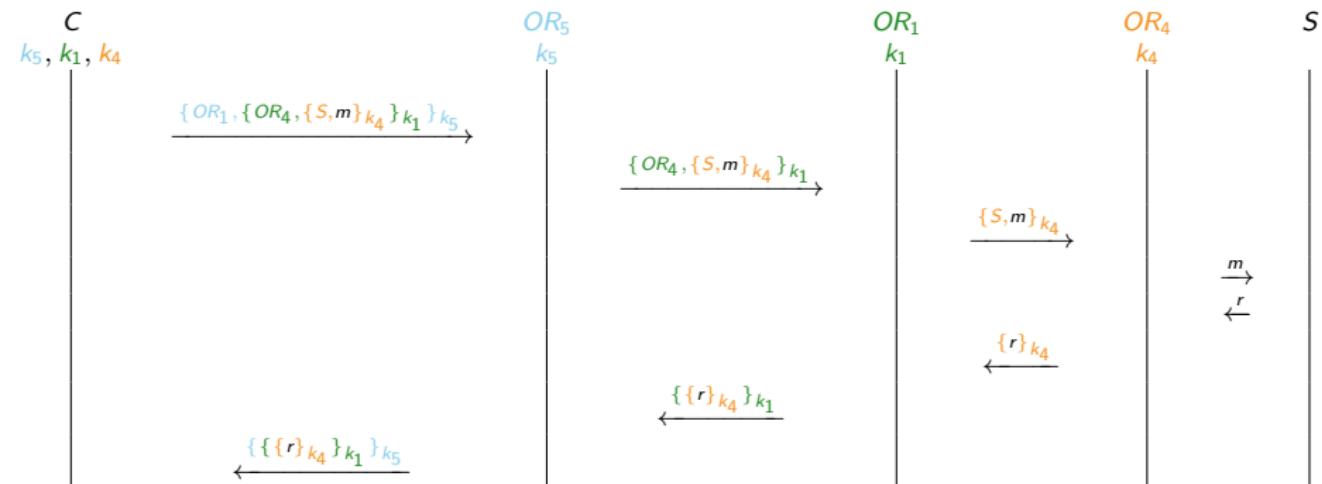
The (simplified) Tor message flow - actual communication



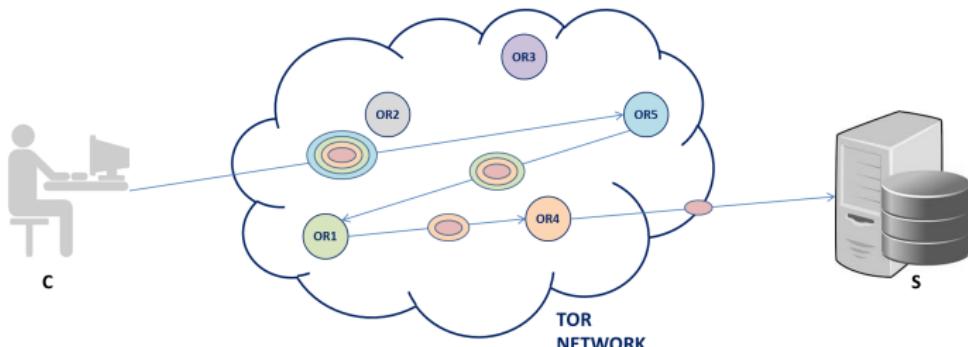
The (simplified) Tor message flow - actual communication



The (simplified) Tor message flow - actual communication

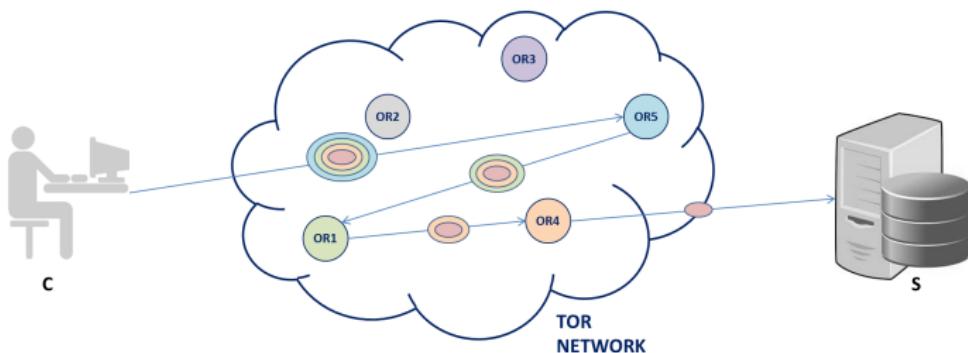


Tor only provides privacy - not confidentiality



- ▶ Tor anonymises the origin of the traffic
- ▶ Tor encrypts everything inside the Tor network
- ▶ but Tor **DOES NOT encrypt all traffic through the Internet**
- ▶ for confidentiality you still need to use end-to-end encryption such as **SSL/TLS**

Tor takes care of DNS resolution

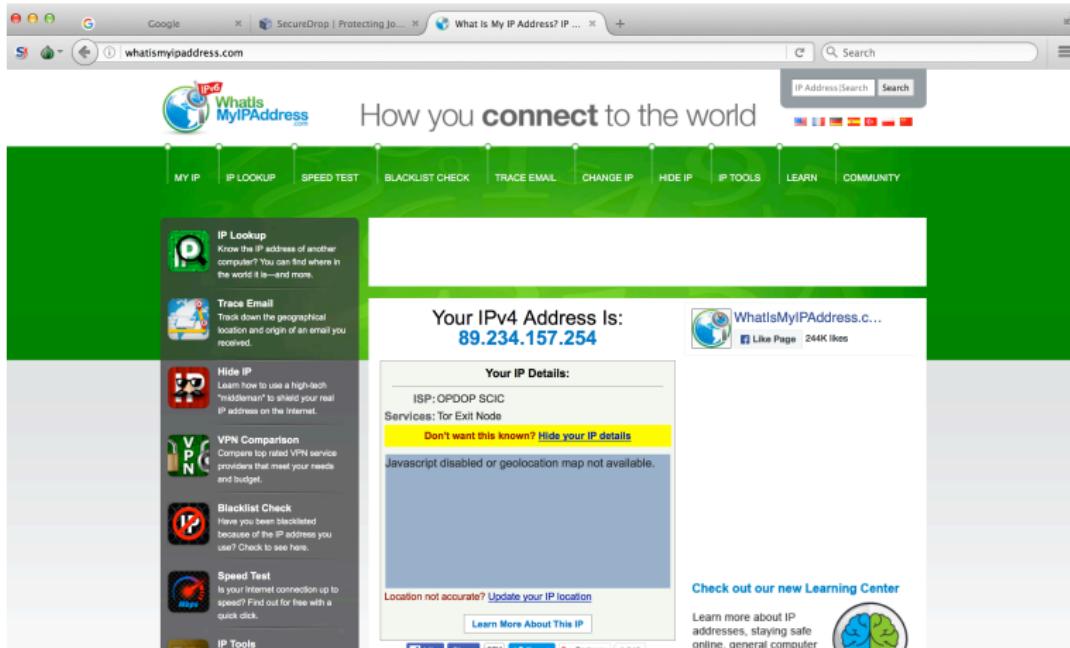


- ▶ Tor only anonymises TCP streams
- ▶ But, DNS resolution is executed over UDP
- ▶ So, DNS resolution if handled by the client browser defeats the purpose of using Tor
- ▶ To avoid privacy breaches due to DNS resolution, the Tor browser delegates DNS resolution to the exit node

Avoiding censorship

- ▶ Tor relays are listed on the public Tor directory
- ▶ So your local ISP can observe that you are communicating with Tor nodes
- ▶ ISPs and governments can try to block access to the Tor network by blocking Tor relays
- ▶ Tor bridge relays are relays not listed on the public Tor directory
- ▶ Entering the Tor network through a Tor bridge relay can prevent ISPs and governments blocking access to the Tor network

The Tor browser



The screenshot shows a web browser window with the URL whatismyipaddress.com in the address bar. The page itself is titled "How you connect to the world". It features a green header with various tools like IP Lookup, Speed Test, and Blacklist Check. The main content area displays the user's IPv4 address as **89.234.157.254**. Below this, there's a section for "Your IP Details:" which includes the ISP (OPDOP SCIC) and Services (Tor Exit Node). A yellow button says "Don't want this known? Hide your IP details". Further down, it says "Javascript disabled or geolocation map not available." At the bottom, there's a link to "Update your IP location" and a "Learn More About This IP" button. To the right, there's a sidebar for the "Learning Center" with a brain icon.

- ▶ whatismyipaddress.com cannot tell where am I using Tor

google.com thinks I'm in the Netherlands using Tor

A screenshot of a Mac OS X desktop showing a Tor Browser window. The browser title bar reads "Tor Browser". The main content area shows a Google search results page for "What Is My IP Address?". A context menu is open over the search results, specifically the "Tor circuit for this site" option under "New Identity". The menu lists several options: "This browser", "United Kingdom (163.172.21.117)", "France (91.121.23.100)", "Netherlands (46.166.148.177)", and "Internet". A yellow banner at the top of the page says "To track you. We recommend that you leave Tor Browser windows in their original default size." At the bottom of the browser window, there are links for "Google-Suche" and "Auf gut Glück!". Below the browser window, the Mac OS X Dock is visible with icons for Finder, Mail, Safari, and others.

New Identity

New Tor Circuit for this Site

Privacy and Security Settings...

Tor Network Settings...

Check for Tor Browser Update...

Tor circuit for this site
(google.de):

- This browser
- United Kingdom (163.172.21.117)
- France (91.121.23.100)
- Netherlands (46.166.148.177)
- Internet

What Is My IP Address? IP ...

OK

Gmail Bilder

Anmelden

Google-Suche

Auf gut Glück!

Google.de angeboten auf: English

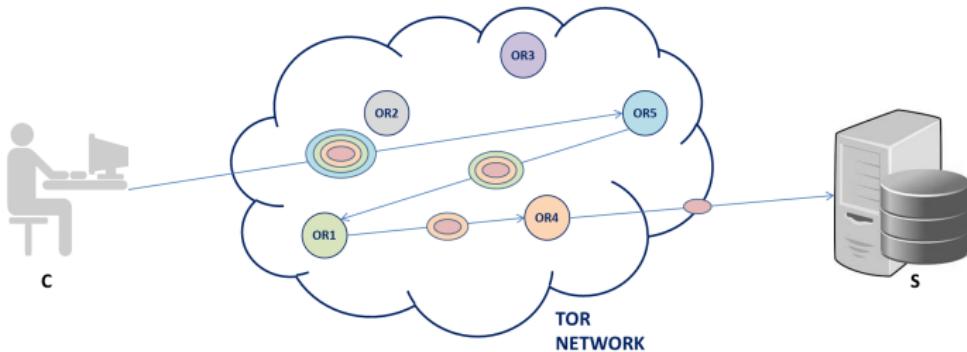
SPÄTER ERINNERN JETZT ANSEHEN

Hinweise zum Datenschutz bei Google

Werbeprogramme Unternehmen Über Google

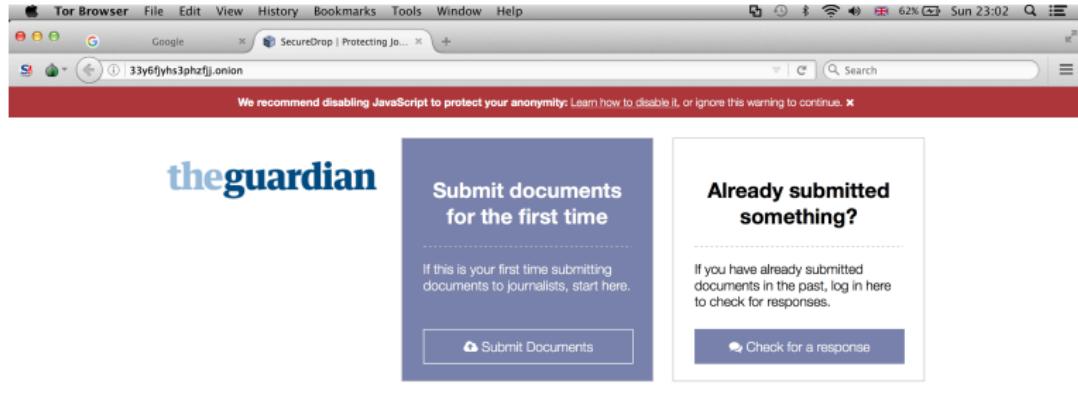
Datenschutzerklärung Nutzungsbedingungen Einstellungen

Limitations of Tor



- ▶ Tor does not provide protection against end-to-end timing attacks
- ▶ If the attacker can see both ends of the communication channel, he can correlate volume and timing information on the two sides

Tor Onion Services



- ▶ Tor can also provide anonymity to websites and servers
- ▶ community.torproject.org/onion-services/overview/

How do Onion Services work?



HSDir



Intro Point

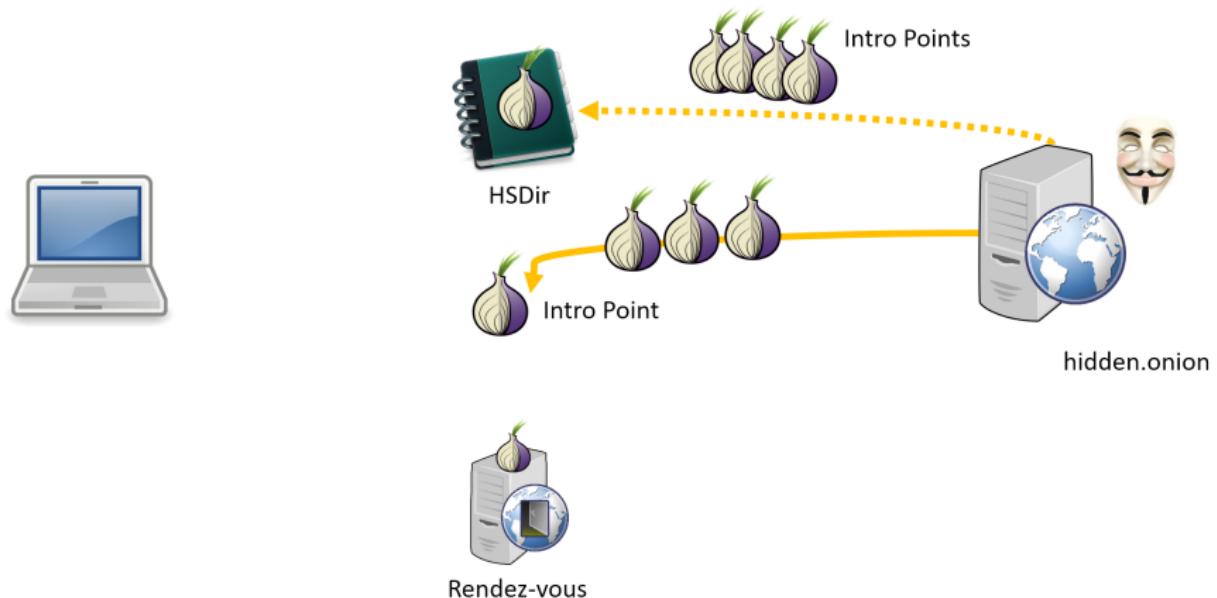


Rendez-vous

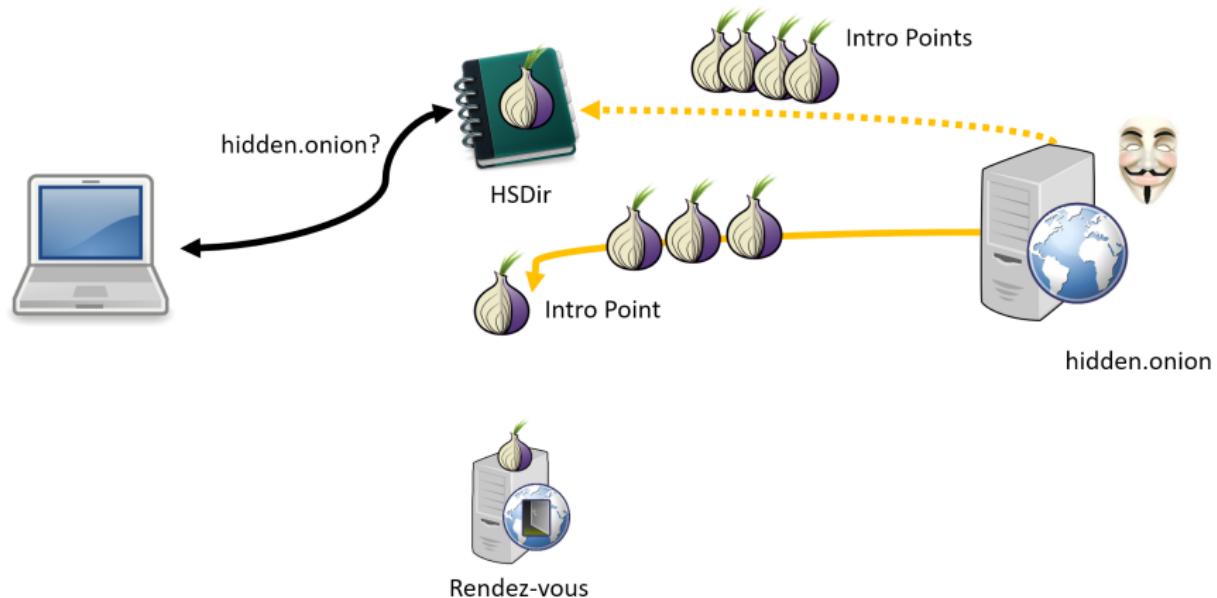


hidden.onion

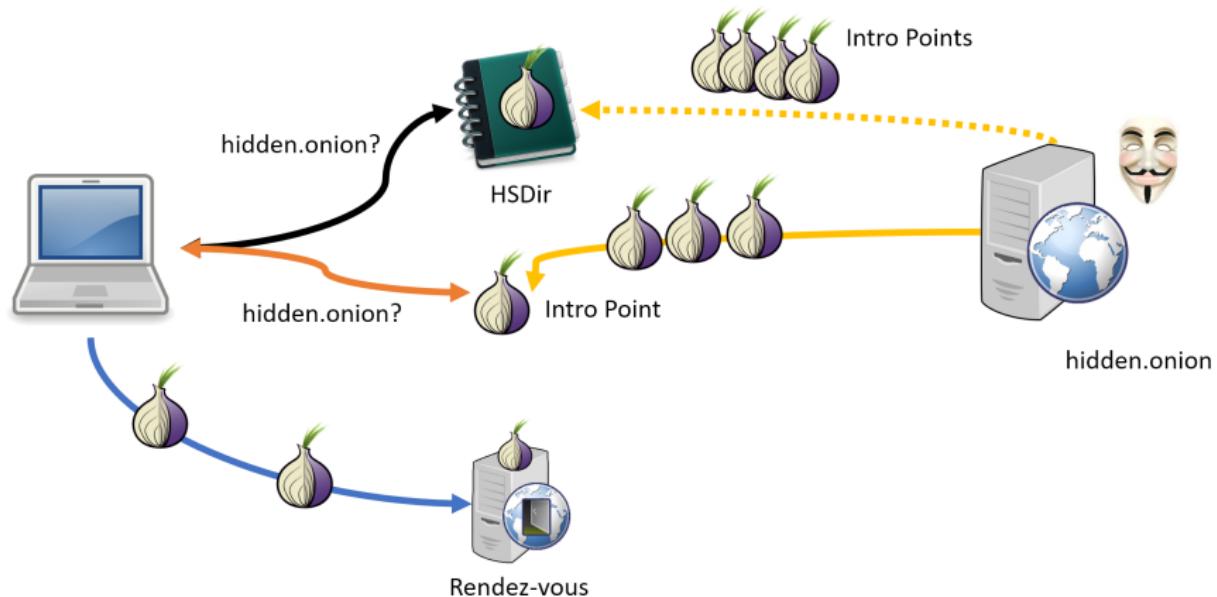
How do Onion Services work?



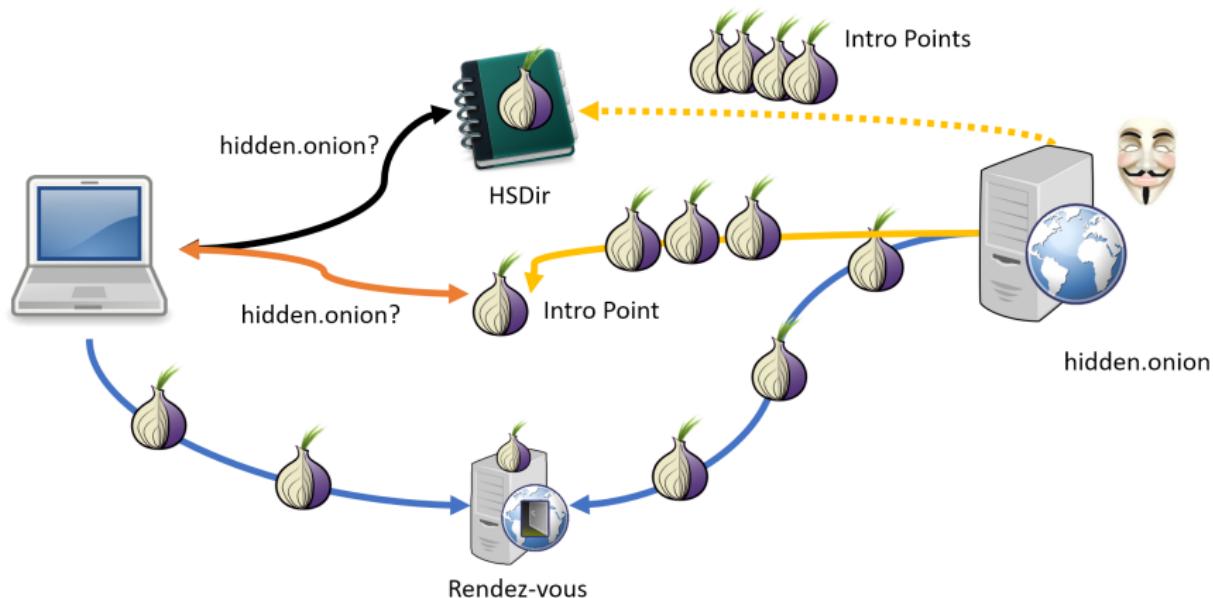
How do Onion Services work?



How do Onion Services work?



How do Onion Services work?



Conclusions

- ▶ Presented a brief overview of several anonymity systems
 - ▶ How they work
 - ▶ Their privacy guarantees
- ▶ Tor
 - ▶ How it works
 - ▶ Tradeoff between privacy and efficiency
- ▶ There is much more to anonymous communications
 - ▶ Tarzan, Bluemoon, etc