

The Tor Protocol

Network Security

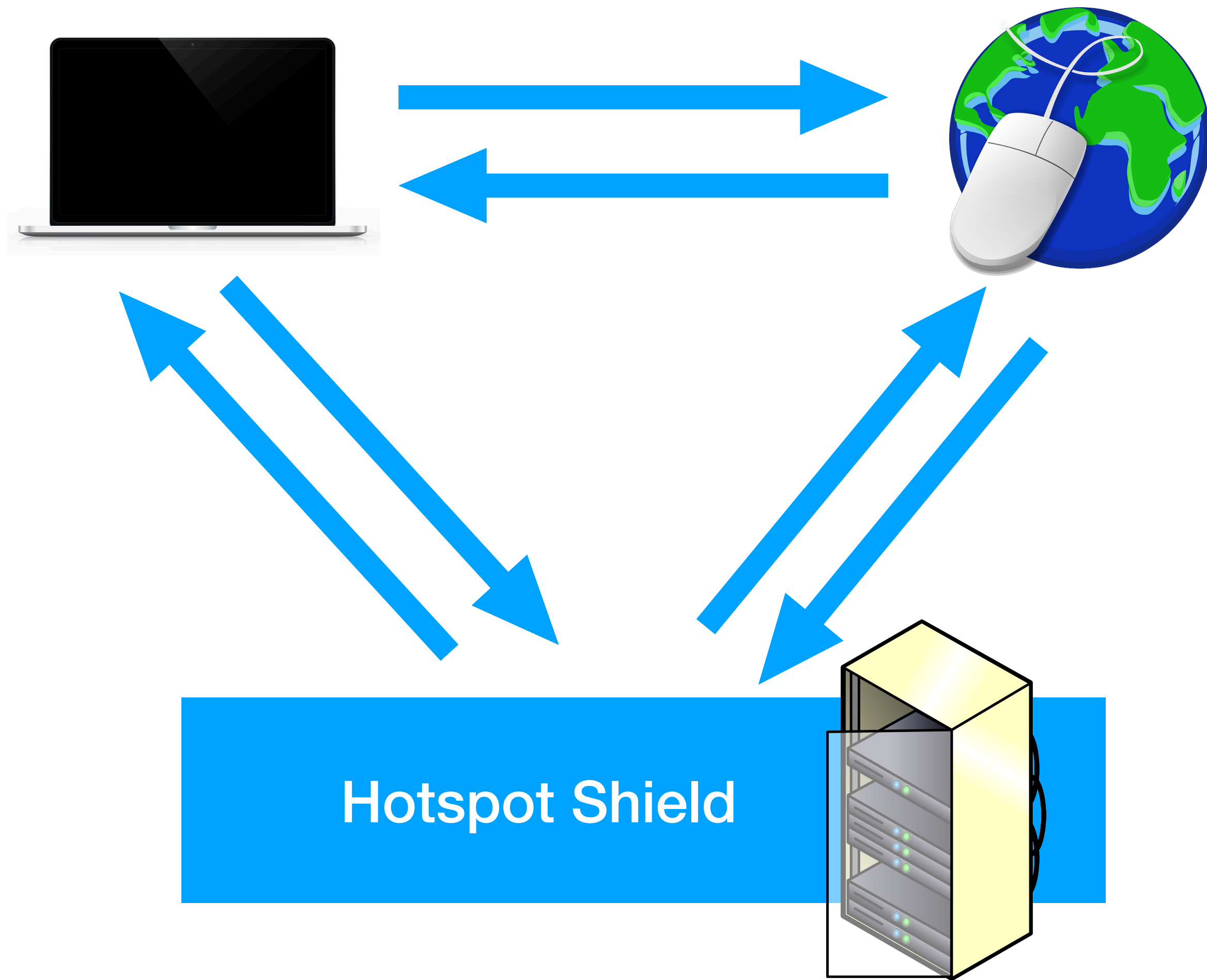
“You have zero privacy anyway, get over it.”

–Scott McNealy, former CEO of SUN Microsystems

“With your permission, you give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about.”

–Eric Schmidt, former CEO of Google

Proxys and VPNs



- An internet connection reveals your IP number.
- VPNs promise “Anonymity”.
- Connection made via their servers.
- The intended recipient server never see’s your IP address.

Virtual Private Networks

- VPNs securely connect you to another network.
- e.g., you can connect to the school's printers via the school's VPN.
- Secured with certificates and encryption, e.g., TLS or IPSec.

Virtual Private Networks For Anonymity

- To get some anonymity, you can route all your traffic via the VPN.
 - Server thinks you are the VPN provider
 - ISP only sees the connection to the VPN
 - A global observer can probably link your connections.
- There is **no anonymity** to the VPN provider.

Virtual Private Networks For Anonymity

- Quiz!
- Suppose you're connected to a public WiFi hotspot and browse to the website "<https://bham.ac.uk>" using a VPN.
- What information does the **WiFi** provider have about you?
 - ...your WiFi's outgoing IP address
 - ...that you are connected to the VPN
 - ...your VPN's outgoing IP address
 - ...that you are browsing to "<https://bham.ac.uk>"
 - ...the contents of your communication with the website

Virtual Private Networks For Anonymity

- Quiz!
- Suppose you're connected to a public WiFi hotspot and browse to the website "<https://bham.ac.uk>" using a VPN.
- What information does the **VPN** provider have about you?
 - ...your WiFi's outgoing IP address
 - ...that you are connected to the VPN
 - ...your VPN's outgoing IP address
 - ...that you are browsing to "<https://bham.ac.uk>"
 - ...the contents of your communication with the website

Virtual Private Networks For Anonymity

- Quiz!
- Suppose you're connected to a public WiFi hotspot and browse to the website "<https://bham.ac.uk>" using a VPN.
- What information does the **website** provider have about you?
 - ...your WiFi's outgoing IP address
 - ...that you are connected to the VPN
 - ...your VPN's outgoing IP address
 - ...that you are browsing to "<https://bham.ac.uk>"
 - ...the contents of your communication with the website


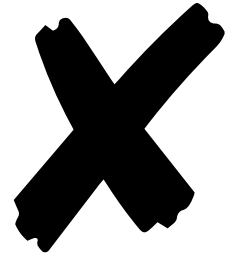



Virtual Private Networks For Anonymity

- Quiz!
- Suppose you're connected to a public WiFi hotspot and browse to the website "<https://bham.ac.uk>" using a VPN.
- What information does the **WiFi** provider have about you?
 - ...your WiFi's outgoing IP address ✓
 - ...that you are connected to the VPN ✓
 - ...your VPN's outgoing IP address ✗
 - ...that you are browsing to "<https://bham.ac.uk>" ✗
 - ...the contents of your communication with the website ✗

Virtual Private Networks For Anonymity

- Quiz!
- Suppose you're connected to a public WiFi hotspot and browse to the website "<https://bham.ac.uk>" using a VPN.
- What information does the **VPN** provider have about you?
 - ...your WiFi's outgoing IP address ✓
 - ...that you are connected to the VPN ✓
 - ...your VPN's outgoing IP address ✓
 - ...that you are browsing to "<https://bham.ac.uk>" ✓
 - ...the contents of your communication with the website ✗

Virtual Private Networks For Anonymity

- Quiz!
- Suppose you're connected to a public WiFi hotspot and browse to the website "<https://bham.ac.uk>" using a VPN.
- What information does the **website** provider have about you?
 - ...your WiFi's outgoing IP address 
 - ...that you are connected to the VPN  Might infer that from the IP address
 - ...your VPN's outgoing IP address 
 - ...that you are browsing to "<https://bham.ac.uk>" 
 - ...the contents of your communication with the website 

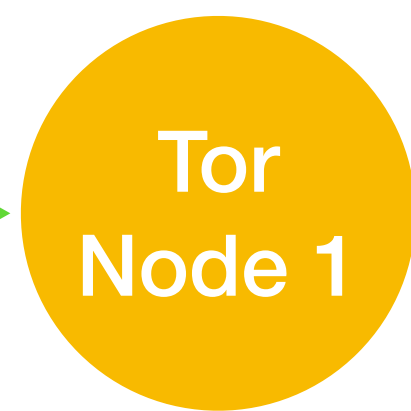
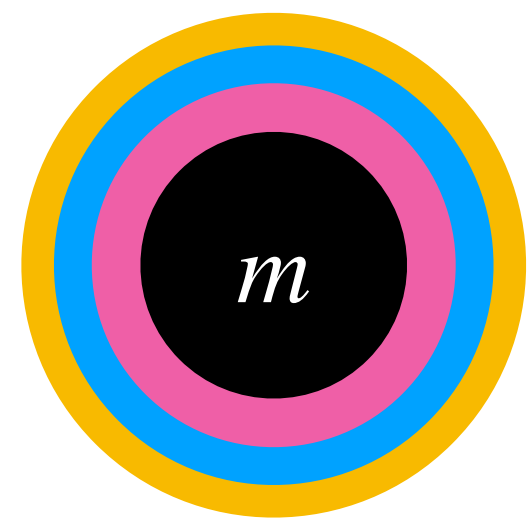
Onion Routing

- You get the best anonymity by routing your traffic via a number of proxies.
- Onion Routing ensures that your message really is routed via the proxies you want.
- The Tor network is using this protocol
<https://www.torproject.org/>

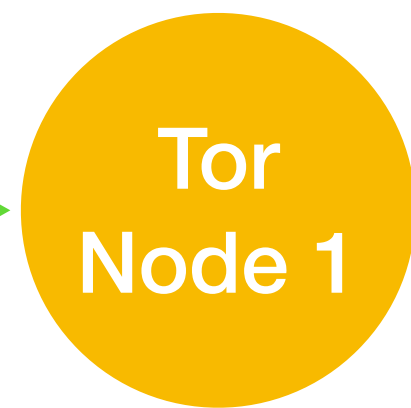
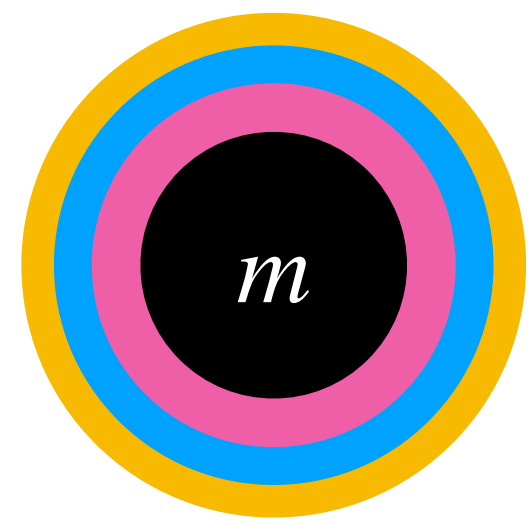
Tor: Onion Routing

- Each proxy only learns the IP of the proxy before it and the proxy after it.
- The public key of each proxy is known.
- Source IP is visible to the first node, destination IP is visible to the last node.
- User picks 3 proxies (entry, middle, and exit node) and is anonymous as long as they aren't all corrupt.

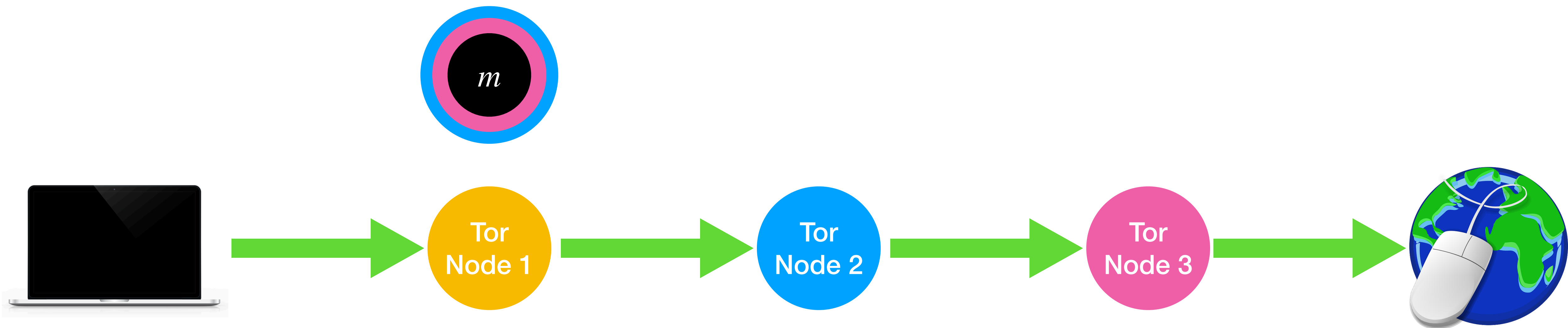
Tor: Onion Routing



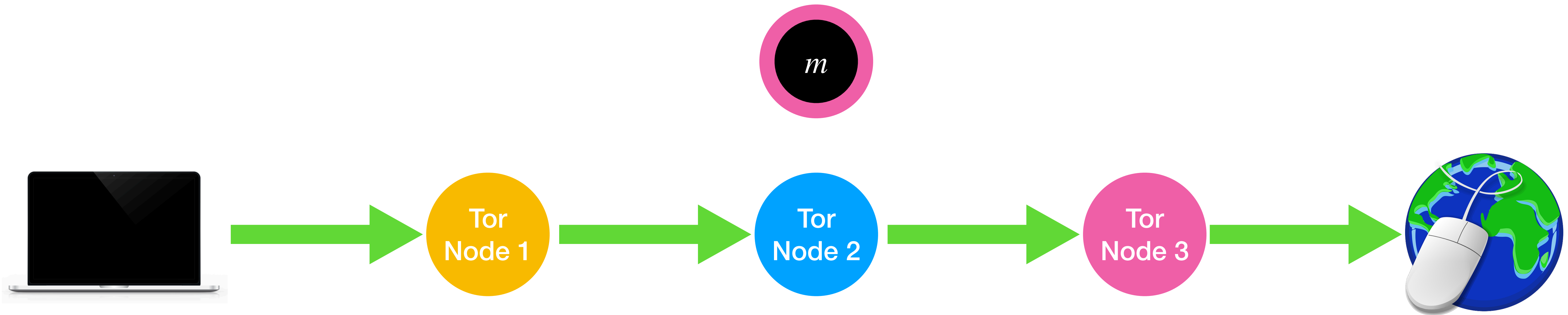
Tor: Onion Routing



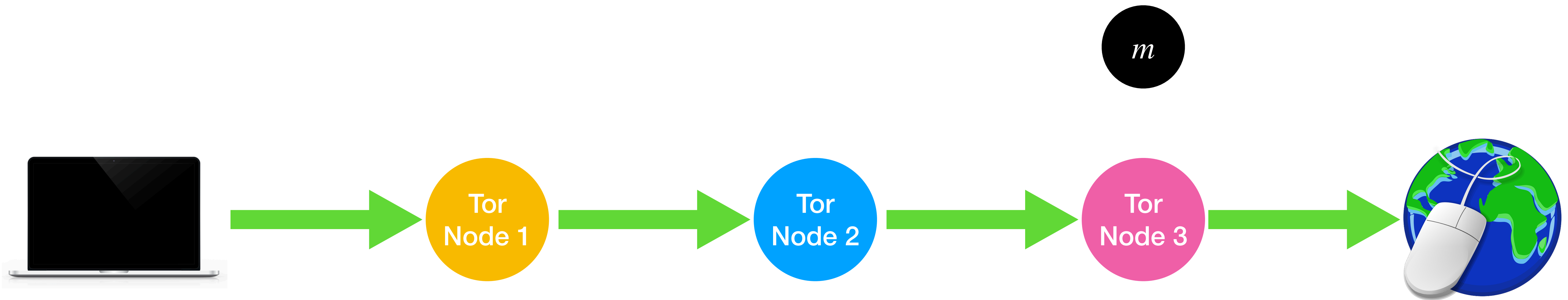
Tor: Onion Routing



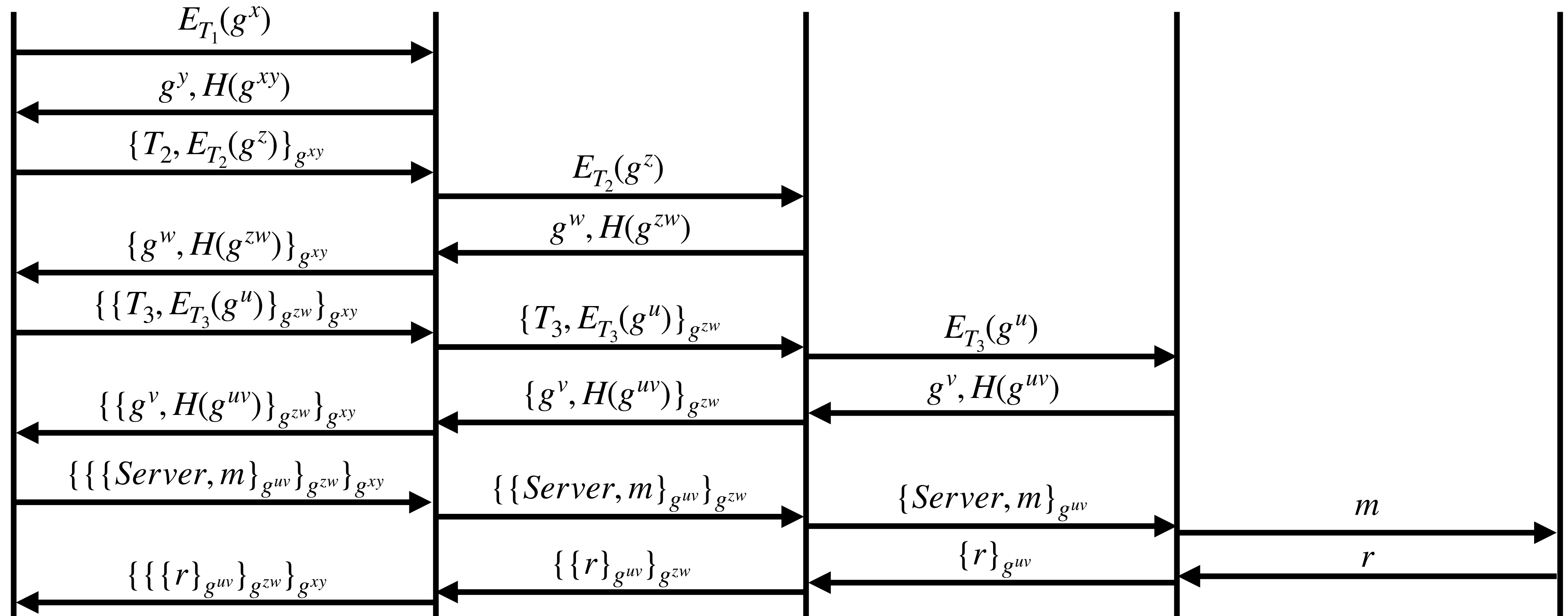
Tor: Onion Routing



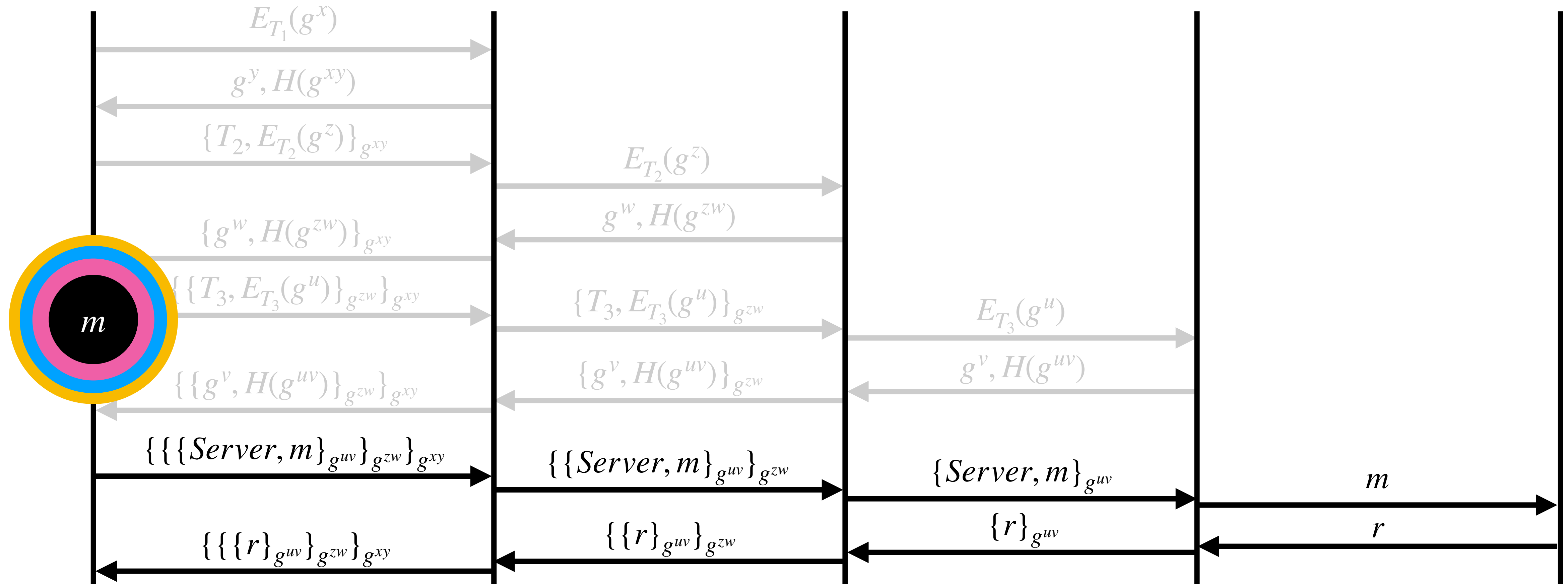
Tor: Onion Routing



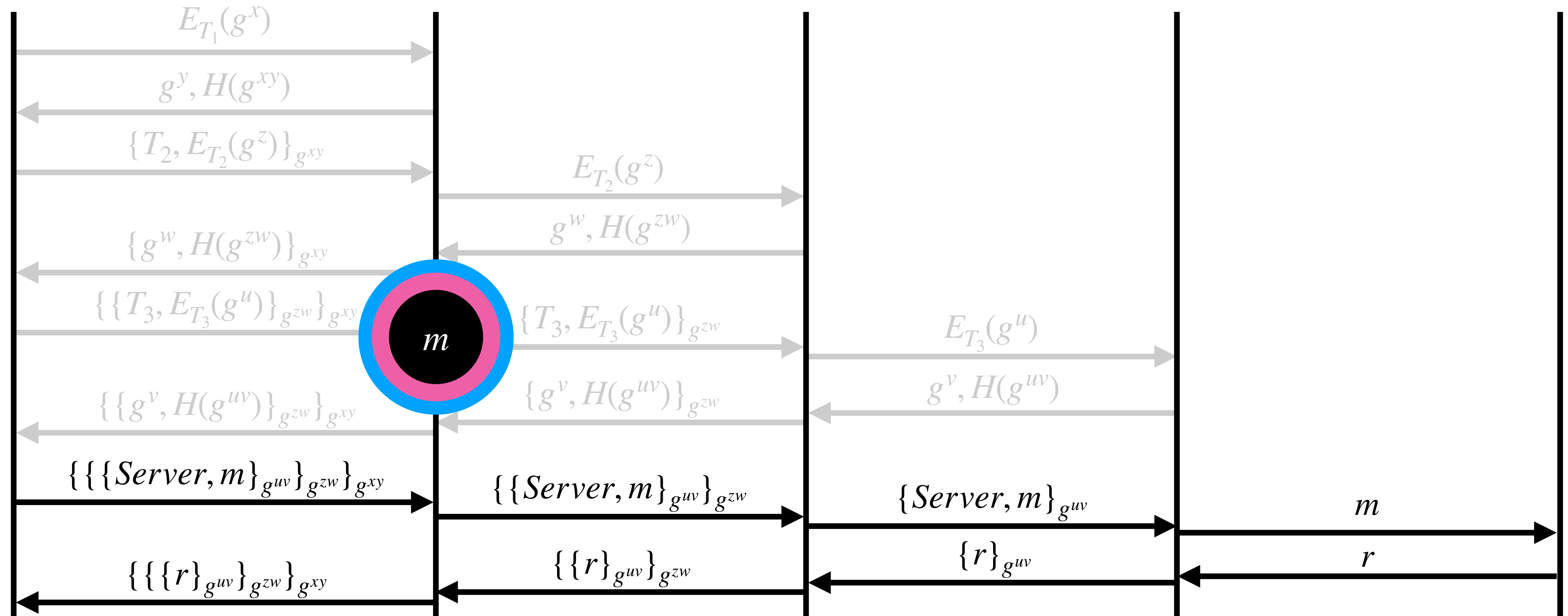
Tor: Onion Routing



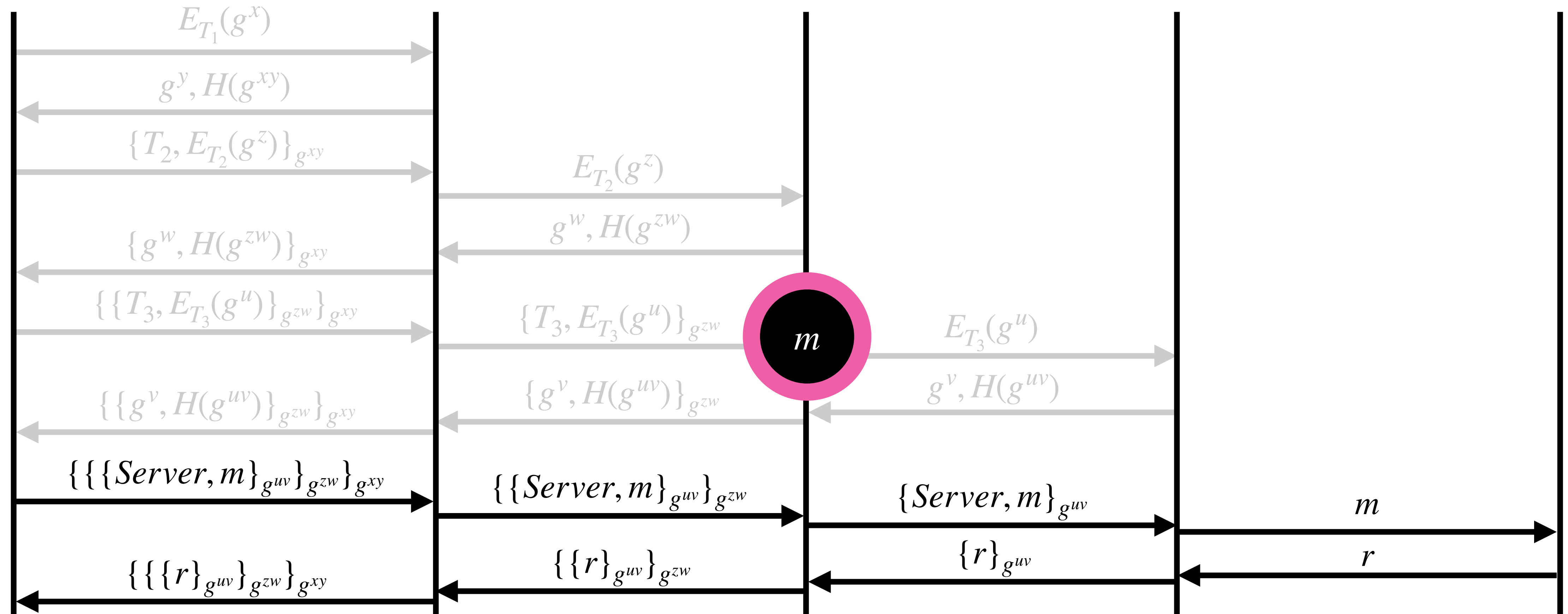
Tor: Onion Routing



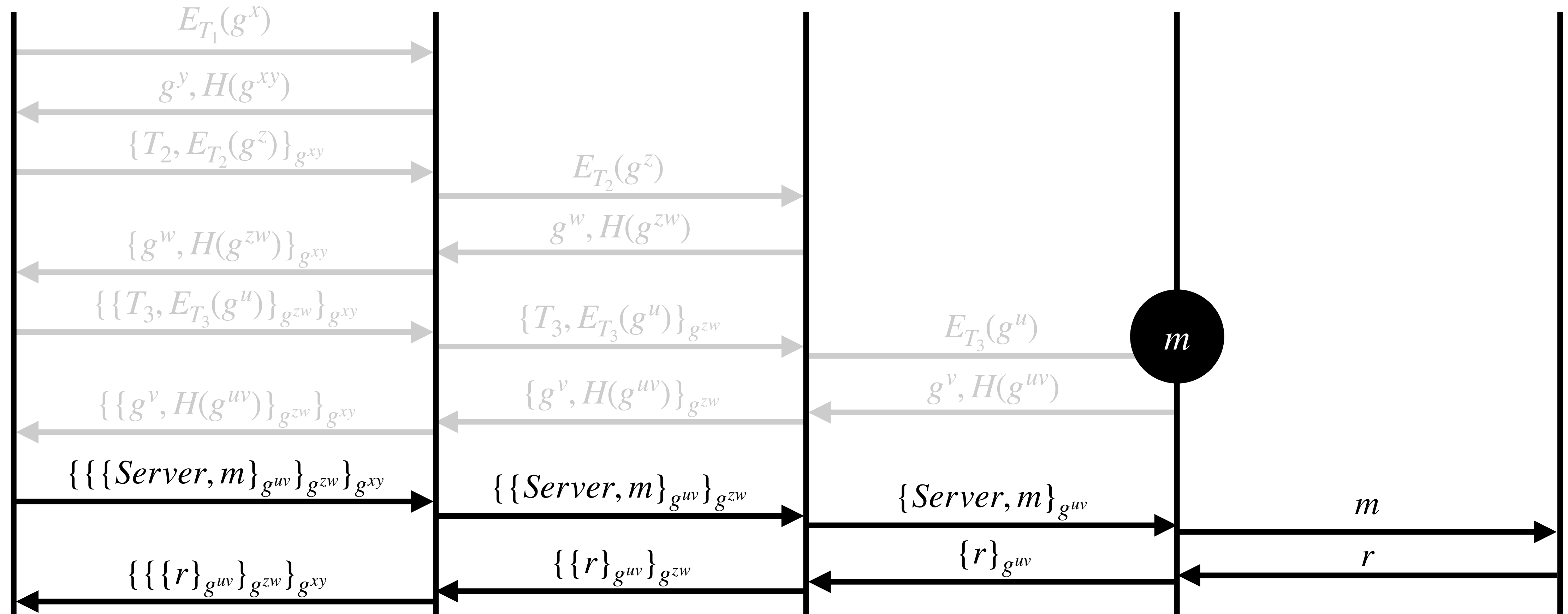
Tor: Onion Routing



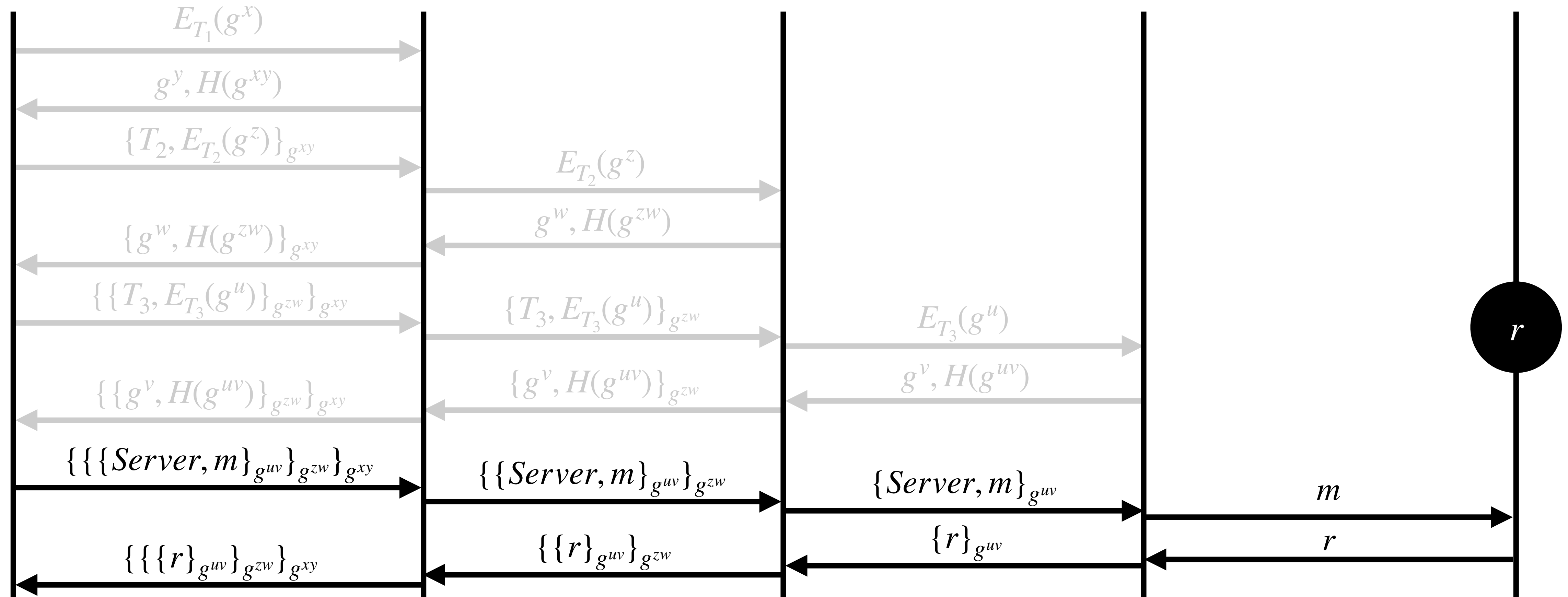
Tor: Onion Routing



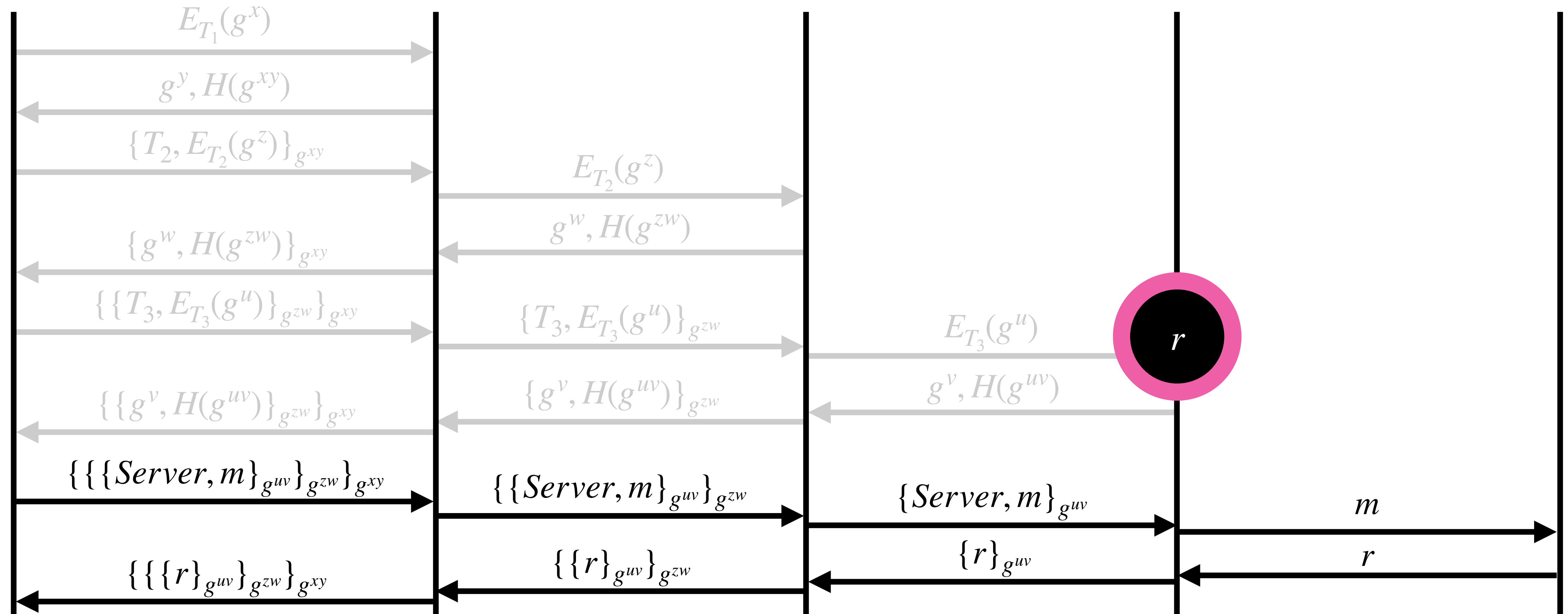
Tor: Onion Routing



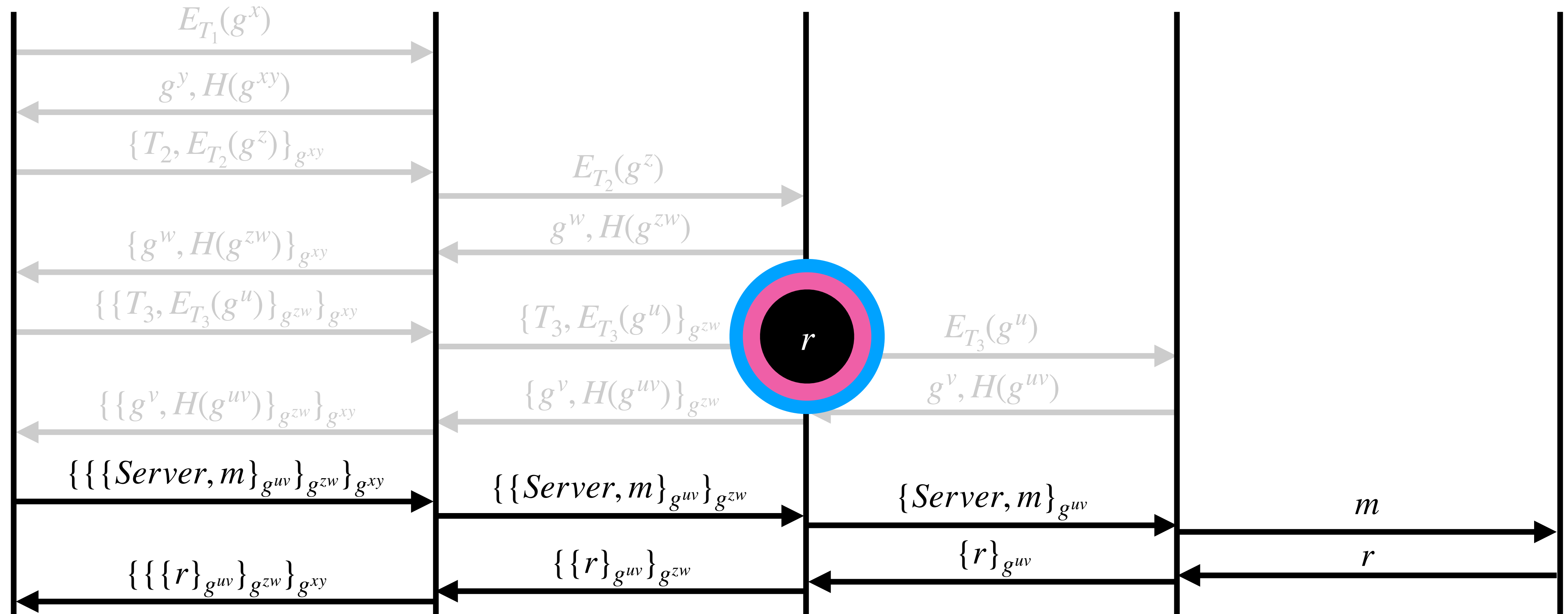
Tor: Onion Routing



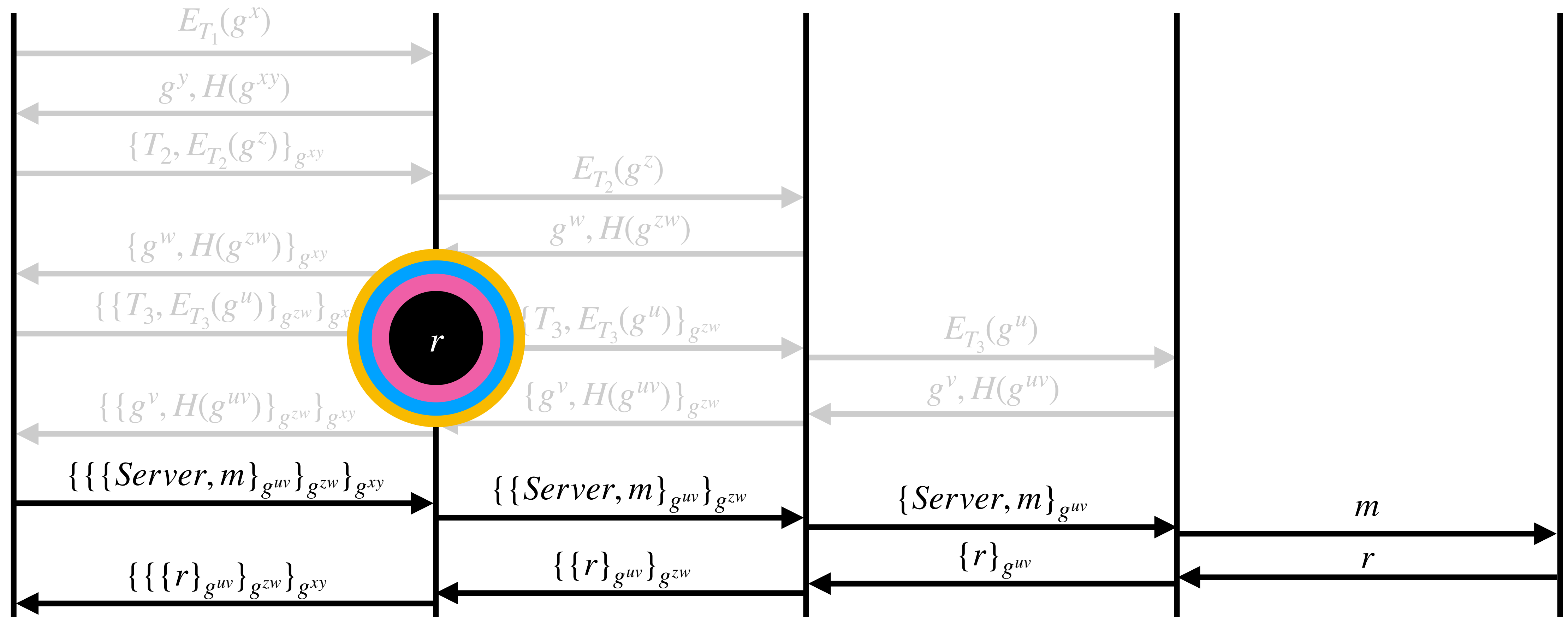
Tor: Onion Routing



Tor: Onion Routing



Tor: Onion Routing

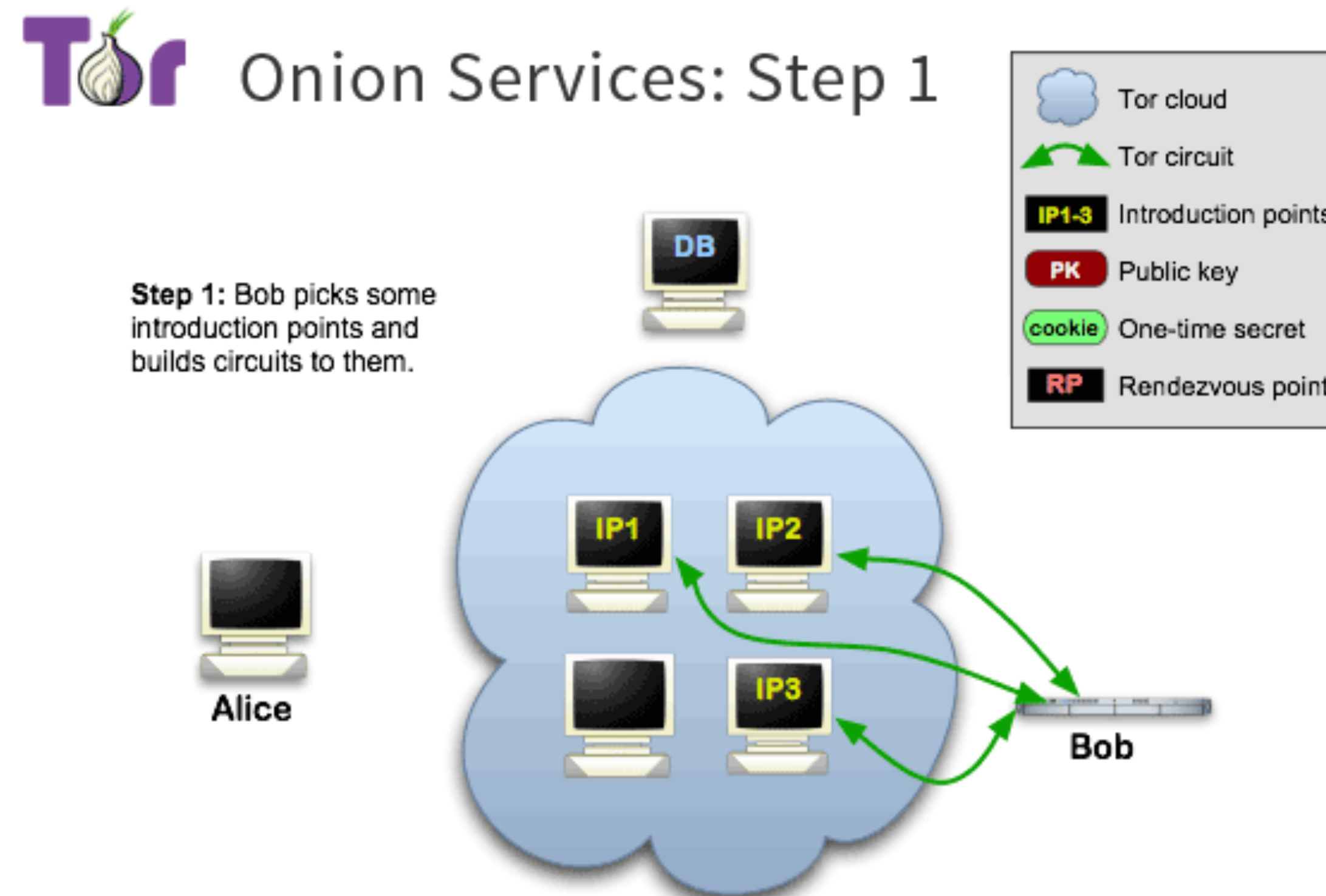


Weaknesses of Tor

- **Traffic analysis** might be possible (timing of requests and responses)
- Some protocols contain **IP addresses** in the messages
- **Exit nodes** can read traffic (if not further protected by TLS, etc.)
- ...

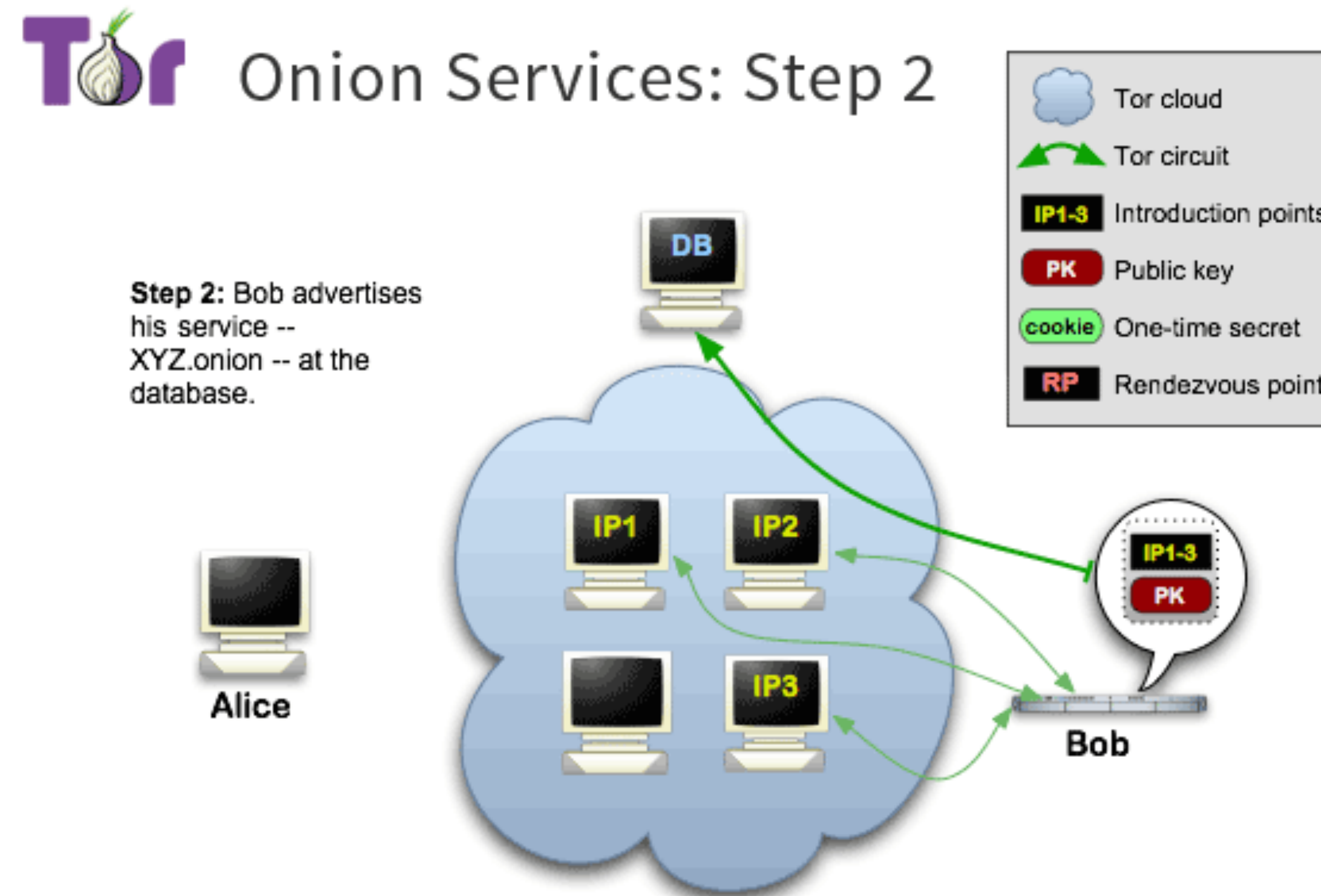
Hidden Servers

- Tor hidden servers hide the server from you.
- See: <https://community.torproject.org/onion-services/overview/>



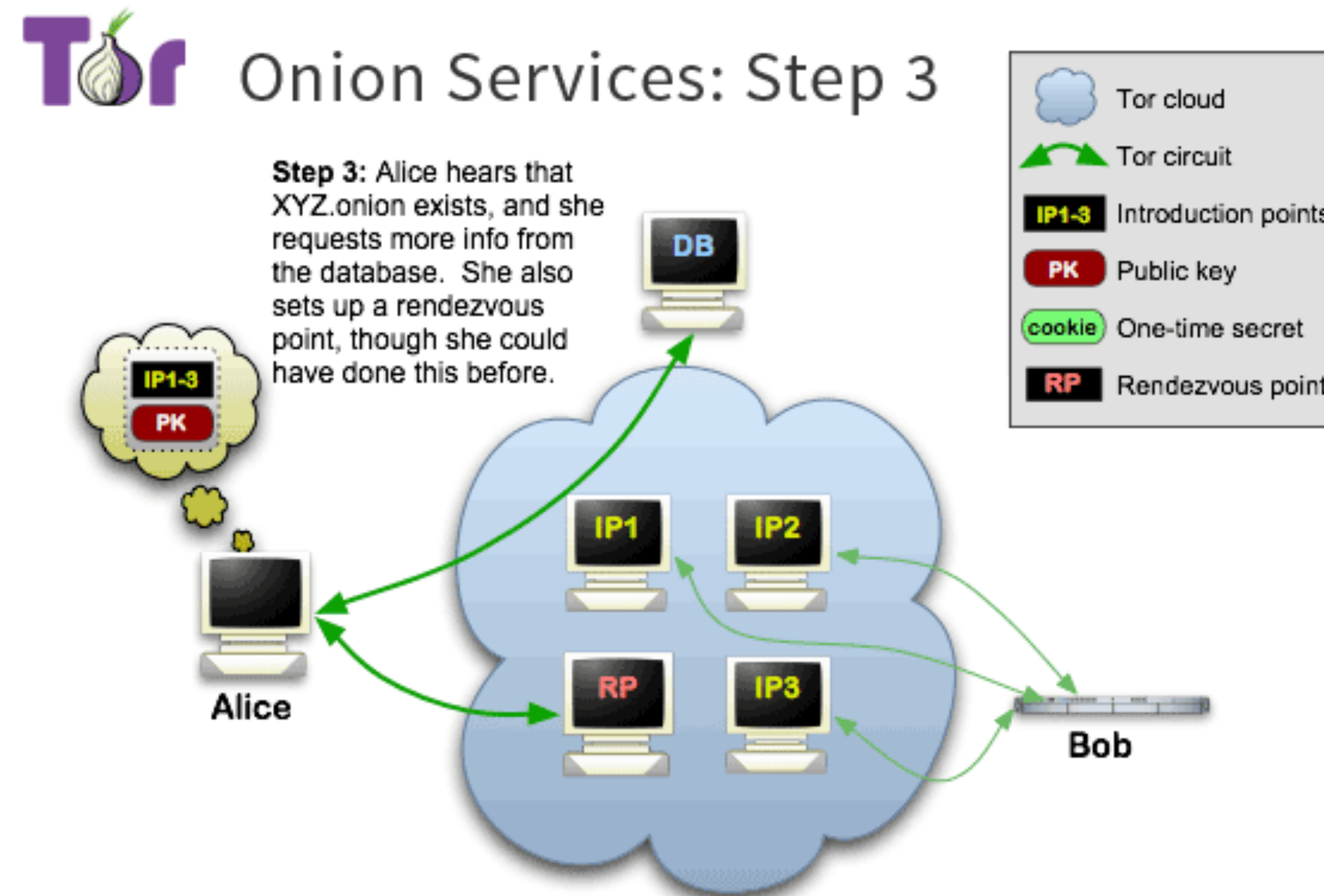
Hidden Servers

- Tor hidden servers hide the server from you.
- See: <https://community.torproject.org/onion-services/overview/>



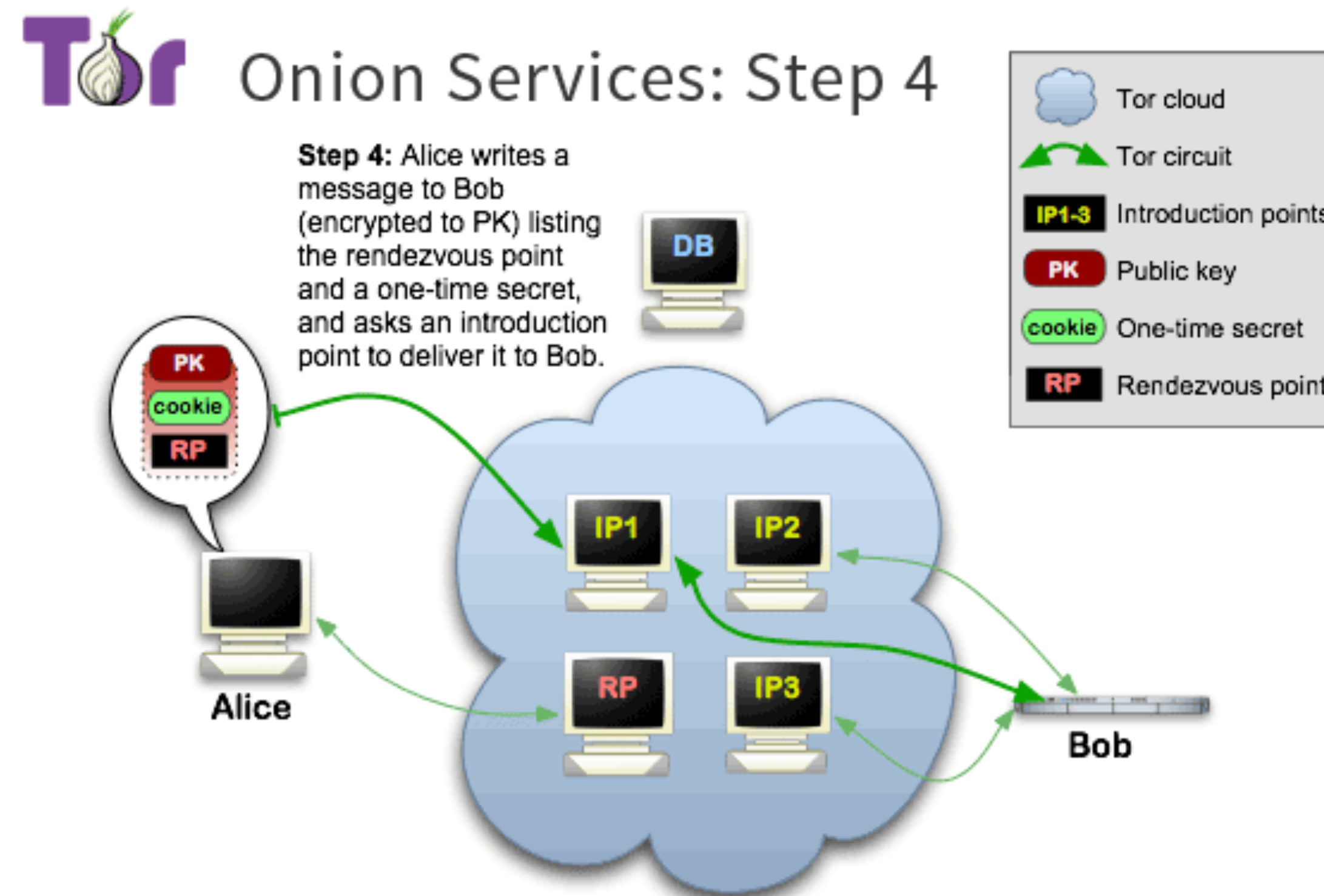
Hidden Servers

- Tor hidden servers hide the server from you.
- See: <https://community.torproject.org/onion-services/overview/>



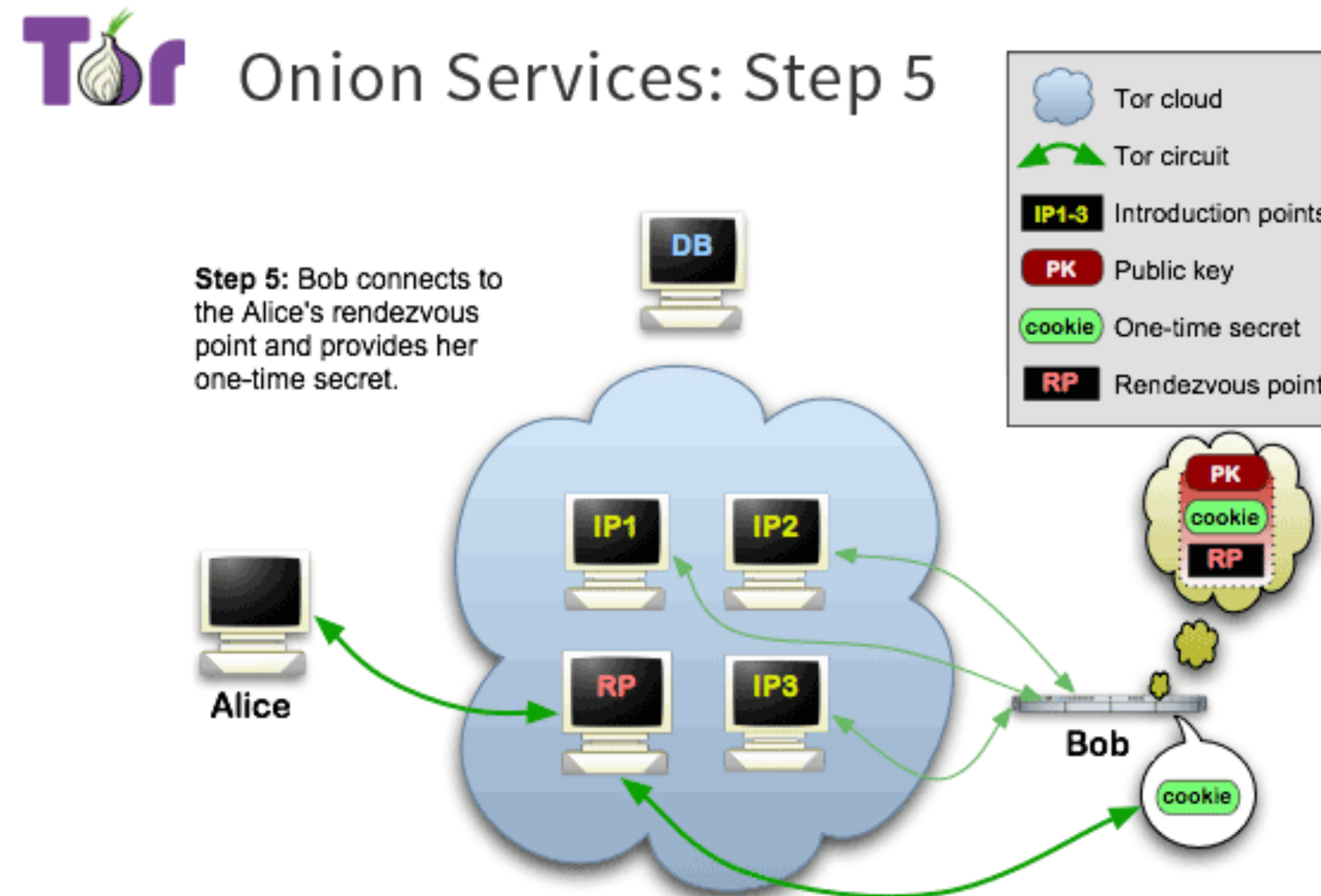
Hidden Servers

- Tor hidden servers hide the server from you.
- See: <https://community.torproject.org/onion-services/overview/>



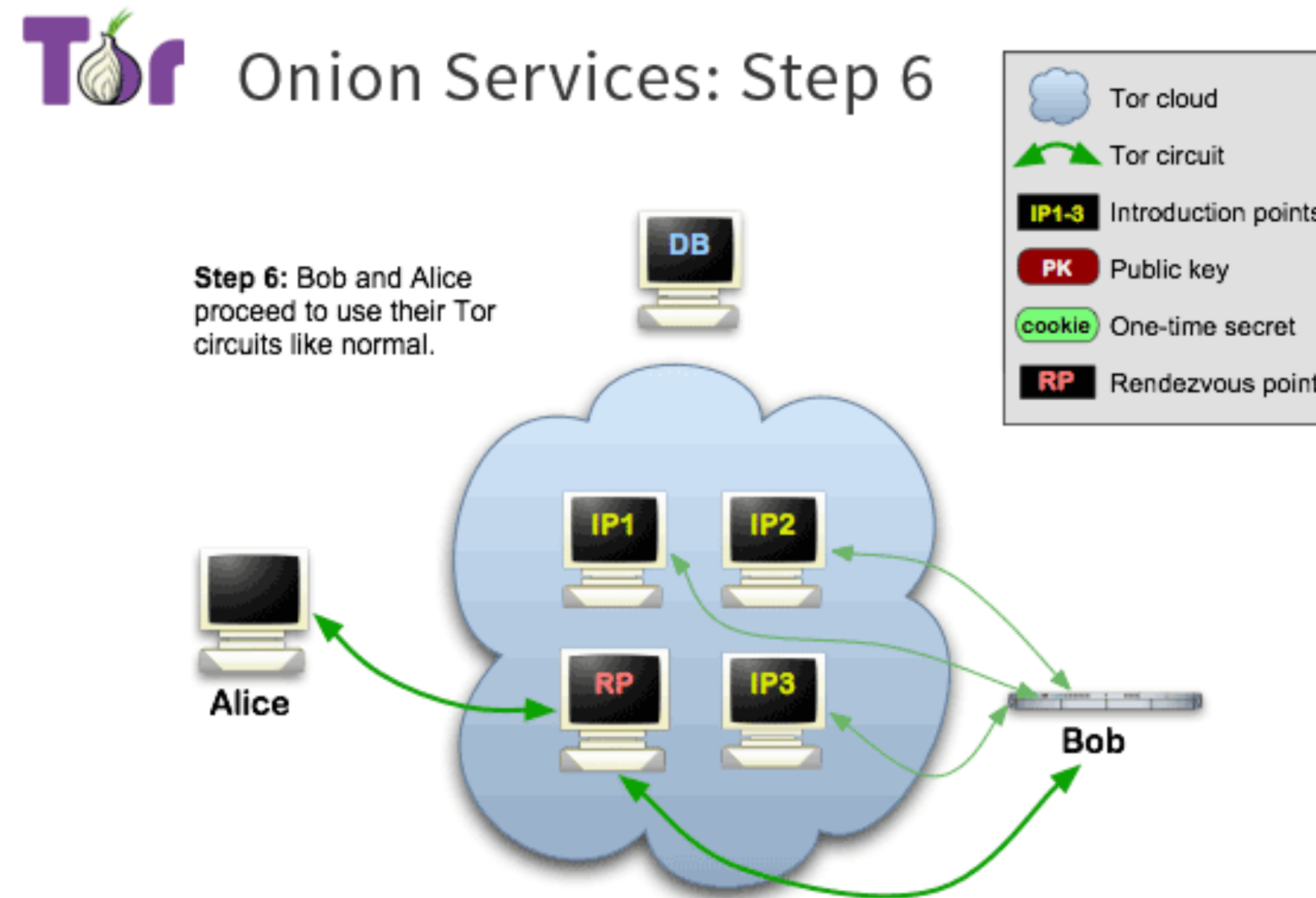
Hidden Servers

- Tor hidden servers hide the server from you.
- See: <https://community.torproject.org/onion-services/overview/>



Hidden Servers

- Tor hidden servers hide the server from you.
- See: <https://community.torproject.org/onion-services/overview/>



Anonymity does not equal security

- The Webservers can still be attacked.
 - e.g., FBI attacked criminal websites running on Tor and implanted malware.
- Poor use of Tor also
 - <http://arstechnica.com/security/2013/12/use-of-tor-helped-fbi-finger-bomb-hoax-suspect/>
 - See warning on: <https://www.theguardian.com/securedrop>

According to federal prosecutors, Tor played a key role in helping FBI agents identify a **Harvard student suspected of e-mailing a hoax bomb threat** to university officials so he wouldn't have to take a final exam. To conceal his Harvard IP address, he used Tor, but in a fatal mistake, he also used the school's Wi-Fi network to connect to the anonymity service. Investigators, according to a **criminal complaint**, took a hard look at everyone who used Tor at the time the threats were sent and ultimately fingered 20-year-old Eldo Kim of Cambridge, Massachusetts as the perpetrator.

While the platform itself uses Tor hidden services to support anonymity, it is advisable to be careful where you access it from. You should avoid using the platform on small networks where use of Tor may be monitored or restricted, or in public places where your screen may be viewed by CCTV. We recommend that you don't jump straight from this landing page to the SecureDrop site, especially on business networks that may be monitored. Best practice would be to make a note of the Tor URL (see below) and then to upload your content from a different machine at a later time.