601.445/601.645
Practical Cryptographic Systems

Tor and Private Browsing

Instructor: Alishah Chator

Housekeeping

- New (last!) assignment coming this week
- Will include written and programming portions
- Project Presentations coming up

This Class so far

- Privacy of content
- Privacy of computation

This Class so far

- Privacy of content
- Privacy of computation
- Where is all of this happening?

This Class so far

- Privacy of content
- Privacy of computation
- Where is all of this happening?
  - Privacy of access?

Setting the stage for Censorship Circumvention

- Make sure no one can read your communications

Setting the stage for Censorship Circumvention

- Make sure no one can read your communications
    - Privacy of content

Setting the stage for Censorship Circumvention

- Make sure no one can read your communications
  - Privacy of content
- Ensuring everyone can access

Setting the stage for Censorship Circumvention

- Make sure no one can read your communications
    - Privacy of content
- Ensuring everyone can access
    - Physical or Monetary access

Setting the stage for Censorship Circumvention

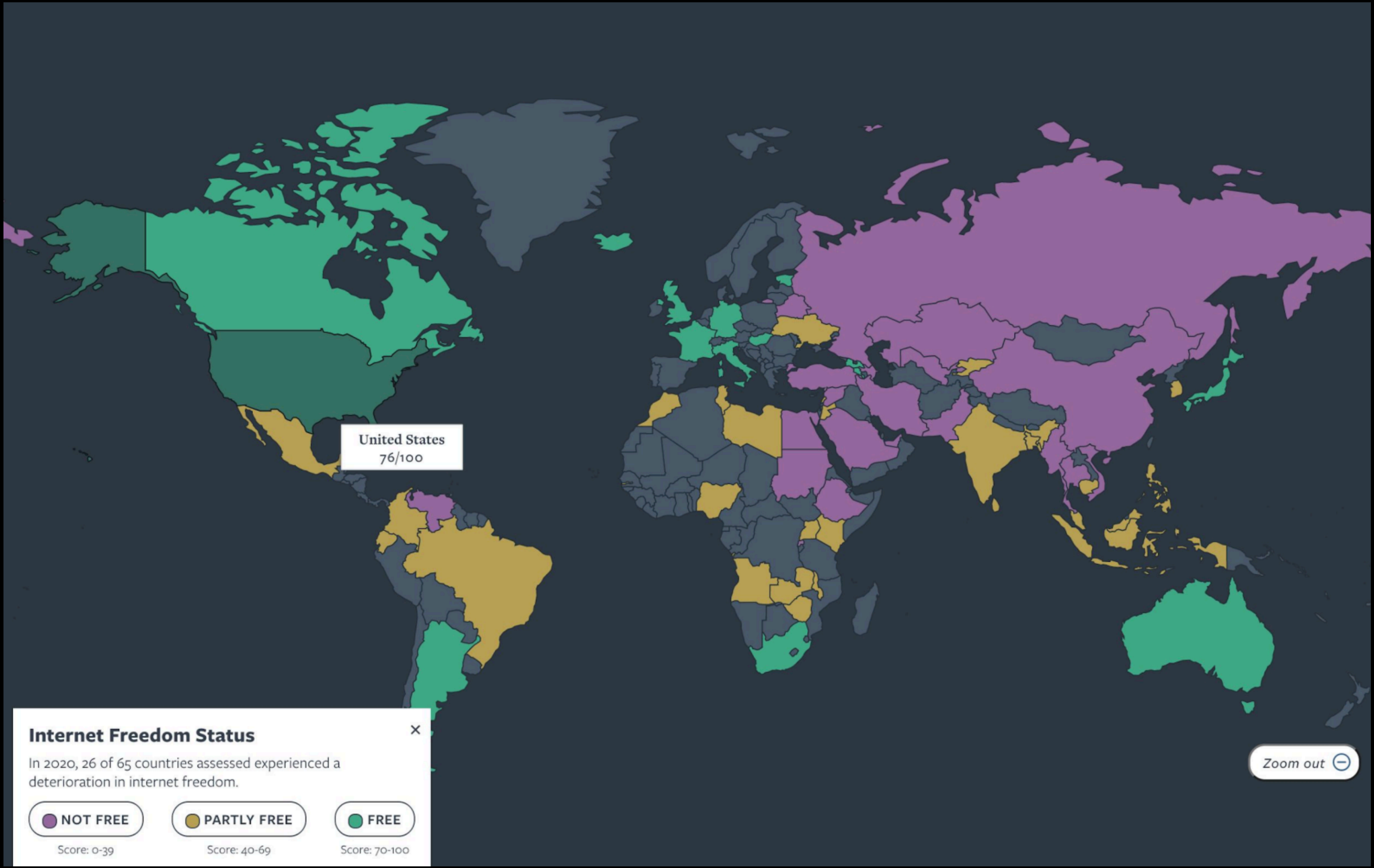
- Make sure no one can read your communications
  - Privacy of content
- Ensuring everyone can access
  - Physical or Monetary access
  - Once you have access, can you use everything?

Setting the stage for Censorship Circumvention

- Make sure no one can read your communications
  - Privacy of content
- Ensuring everyone can access
  - Physical or Monetary access
  - **Goal:** Once you have access, can you use everything?

Setting the stage for Censorship Circumvention

- Make sure no one can read your communications
  - Privacy of content
- Ensuring everyone can access
  - Physical or Monetary access
  - **Goal:** Once you have access, can you use everything?
    - Privacy on the internet



Internet Freedom Status

In 2020, 26 of 65 countries assessed experienced a deterioration in internet freedom.

● NOT FREE	● PARTLY FREE	● FREE
Score: 0-39	Score: 40-69	Score: 70-100

Data Vs Metadata

Data Vs Metadata

Data

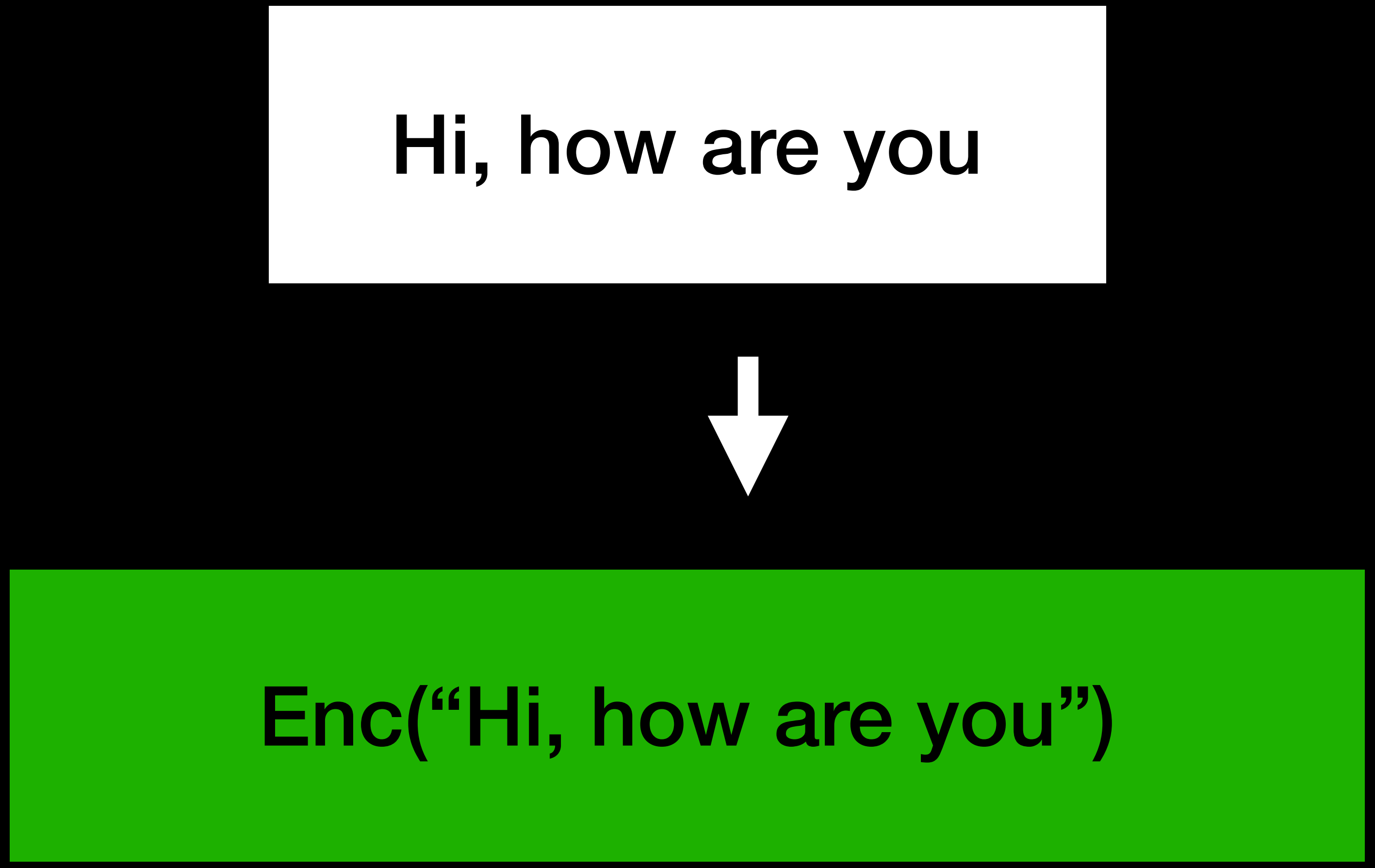
Data Vs Metadata

Data

Hi, how are you

Data Vs Metadata

Data



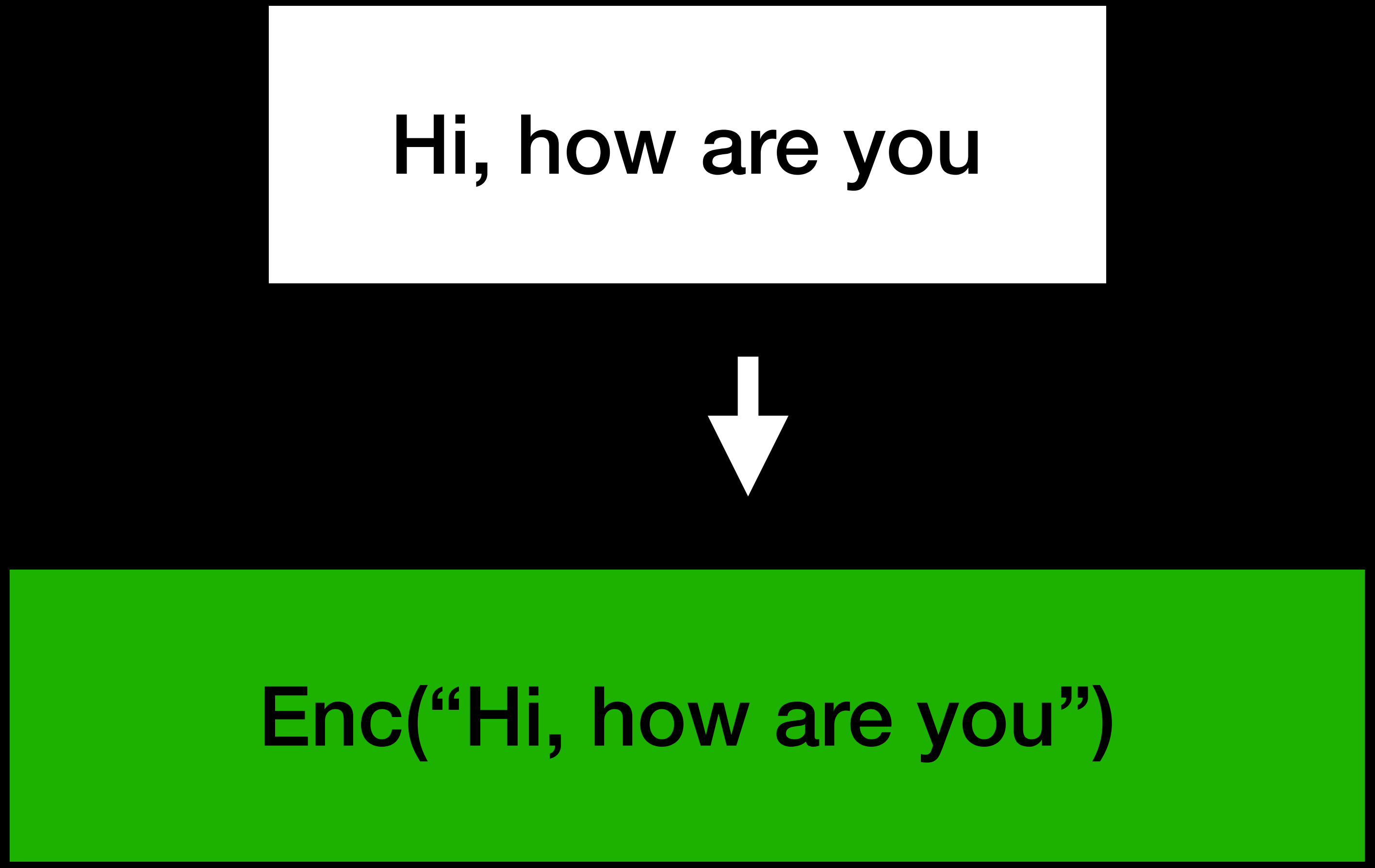
Hi, how are you

↓

Enc(“Hi, how are you”)

Data Vs Metadata

Data



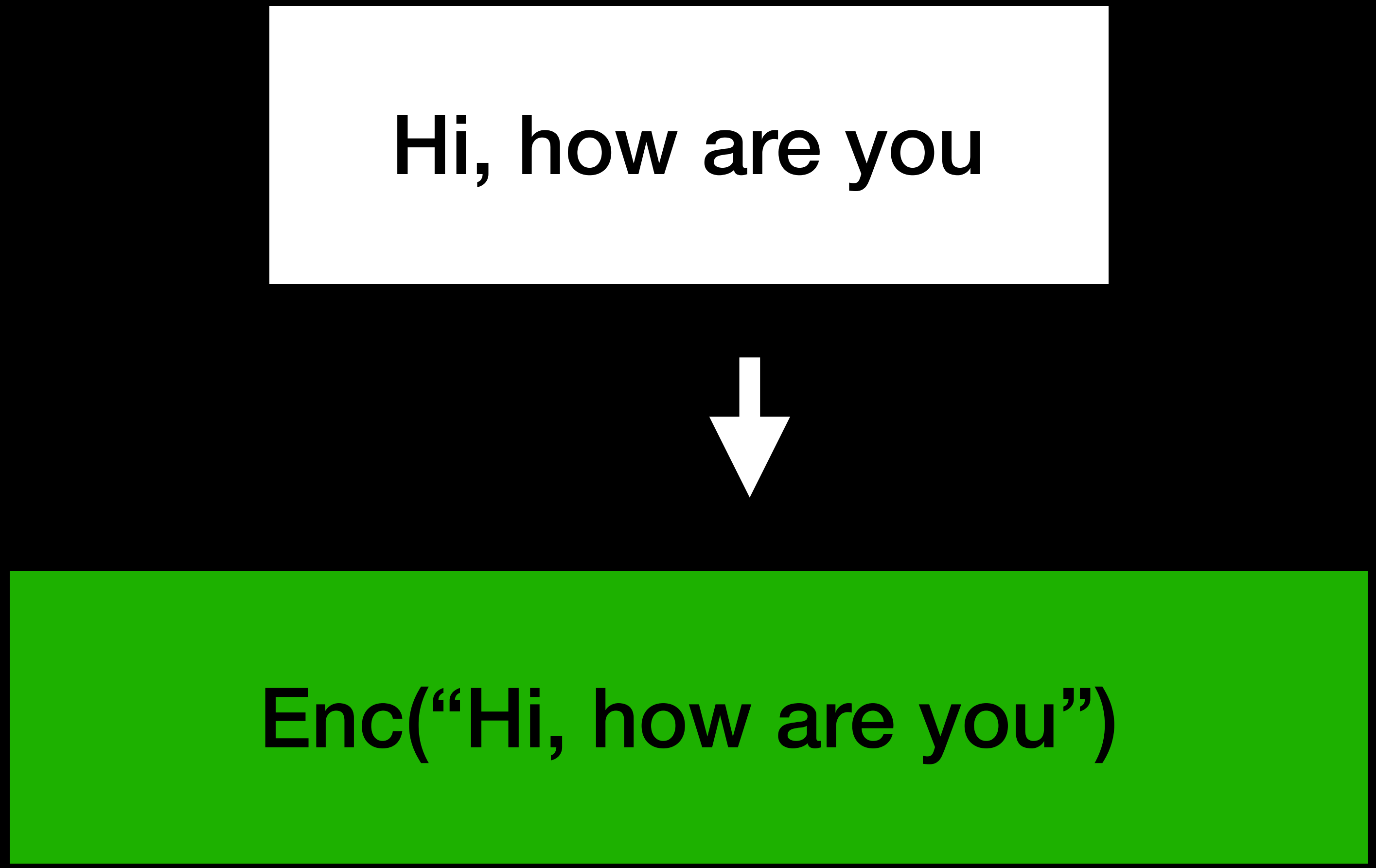
Hi, how are you

Enc(“Hi, how are you”)

Metadata

Data Vs Metadata

Data



Hi, how are you

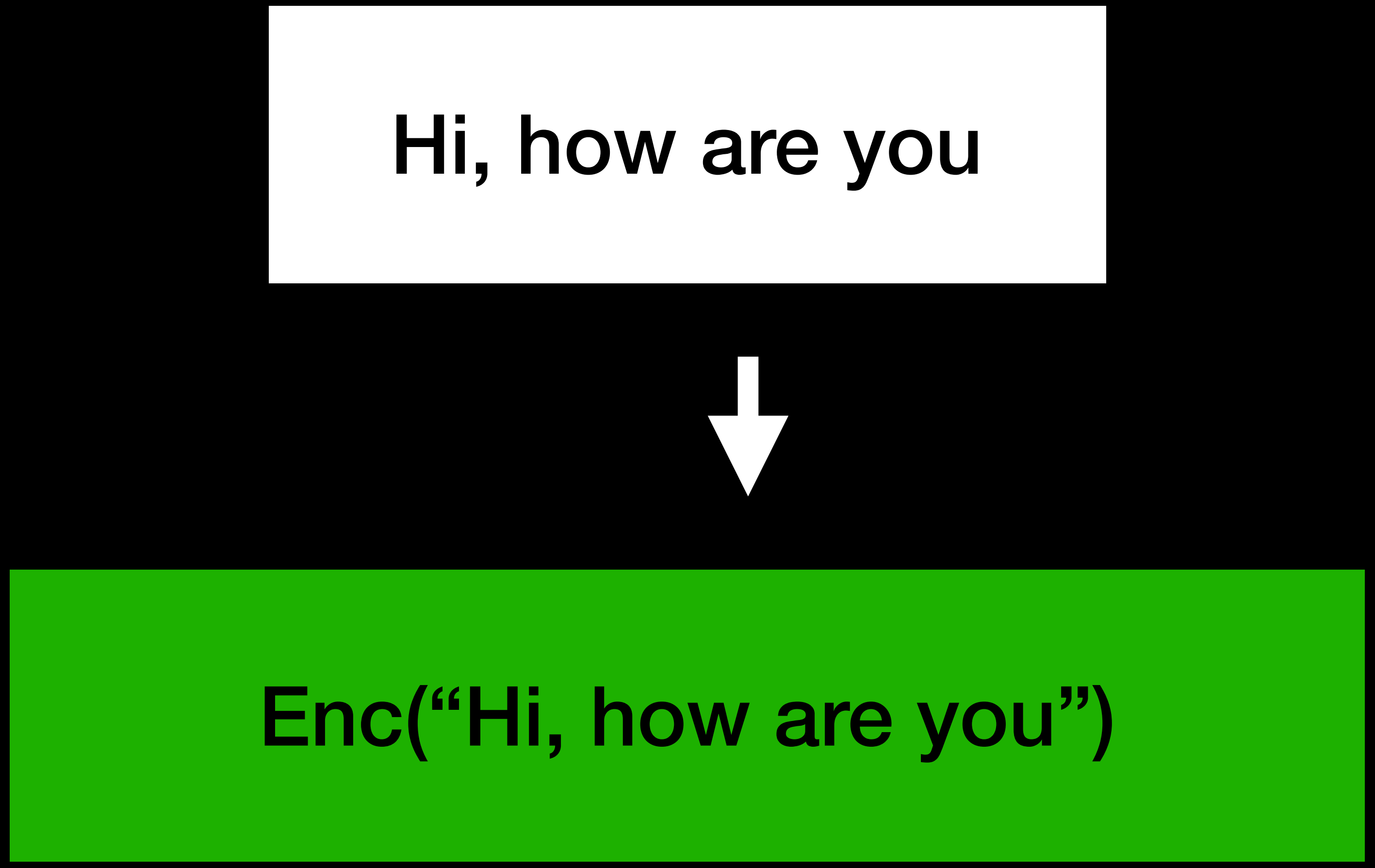
Enc(“Hi, how are you”)

Metadata

- Who is this for
- Who is this from
- Timestamps

Data Vs Metadata

Data



Hi, how are you

Enc(“Hi, how are you”)

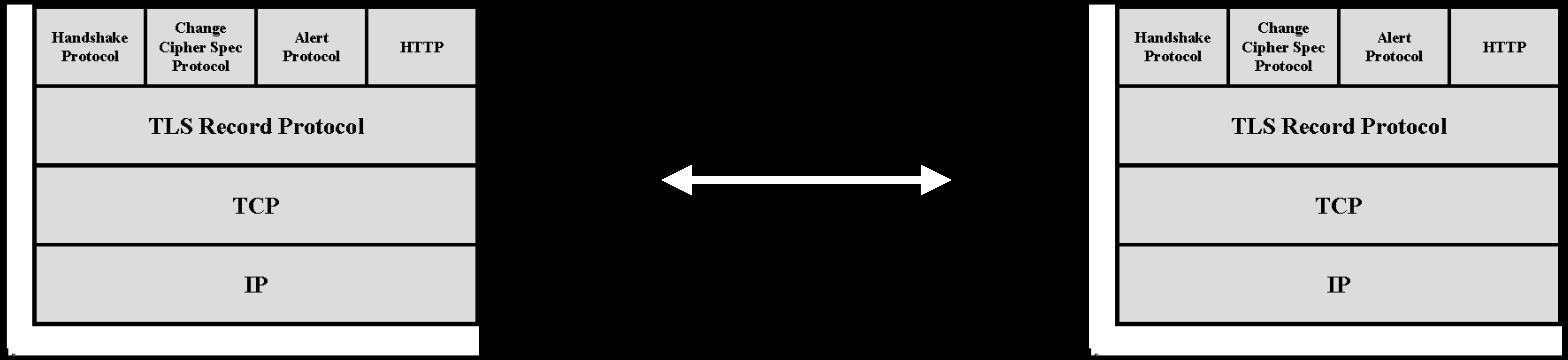
Metadata

- Who is this for
- Who is this from
- Timestamps

All of this is cleartext!

“We kill people based on metadata.”

Internet Metadata Leakage



Handshake Protocol | Change Cipher Spec Protocol | Alert Protocol | HTTP

TLS Record Protocol

TCP

IP

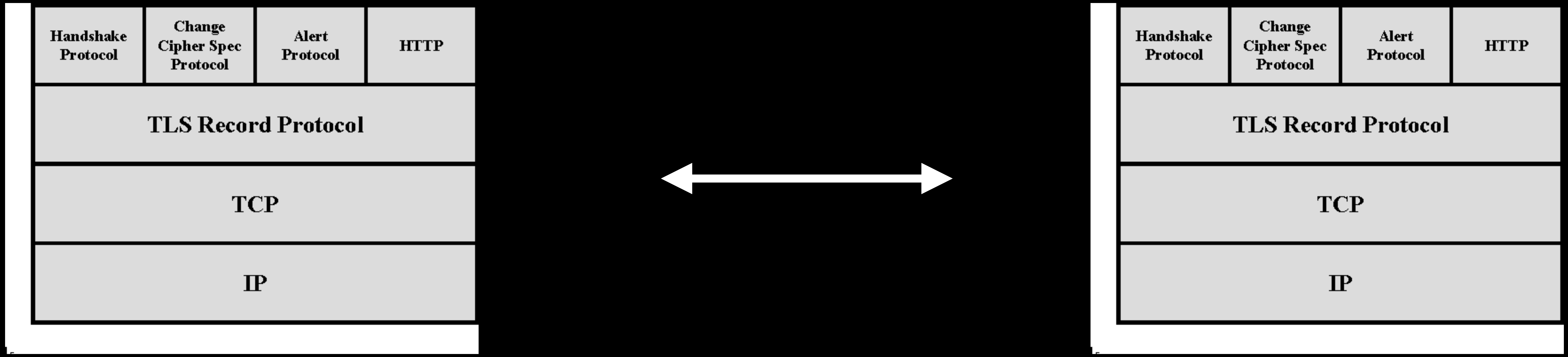
Handshake Protocol | Change Cipher Spec Protocol | Alert Protocol | HTTP

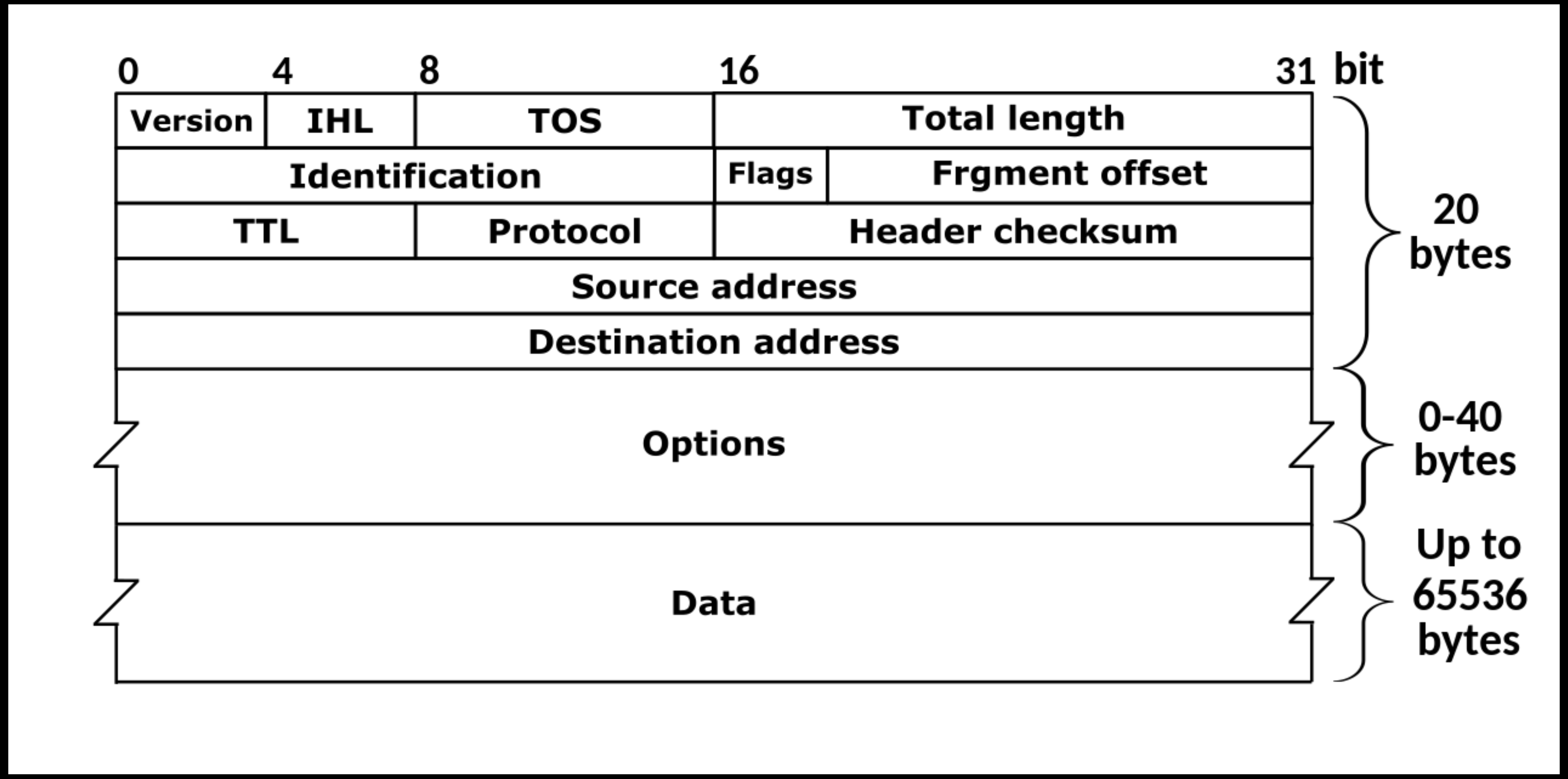
TLS Record Protocol

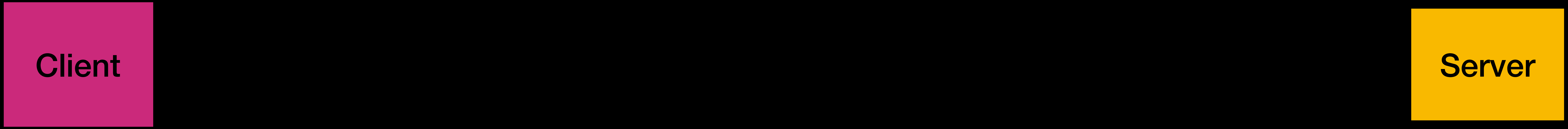
TCP

IP

Internet Metadata Leakage

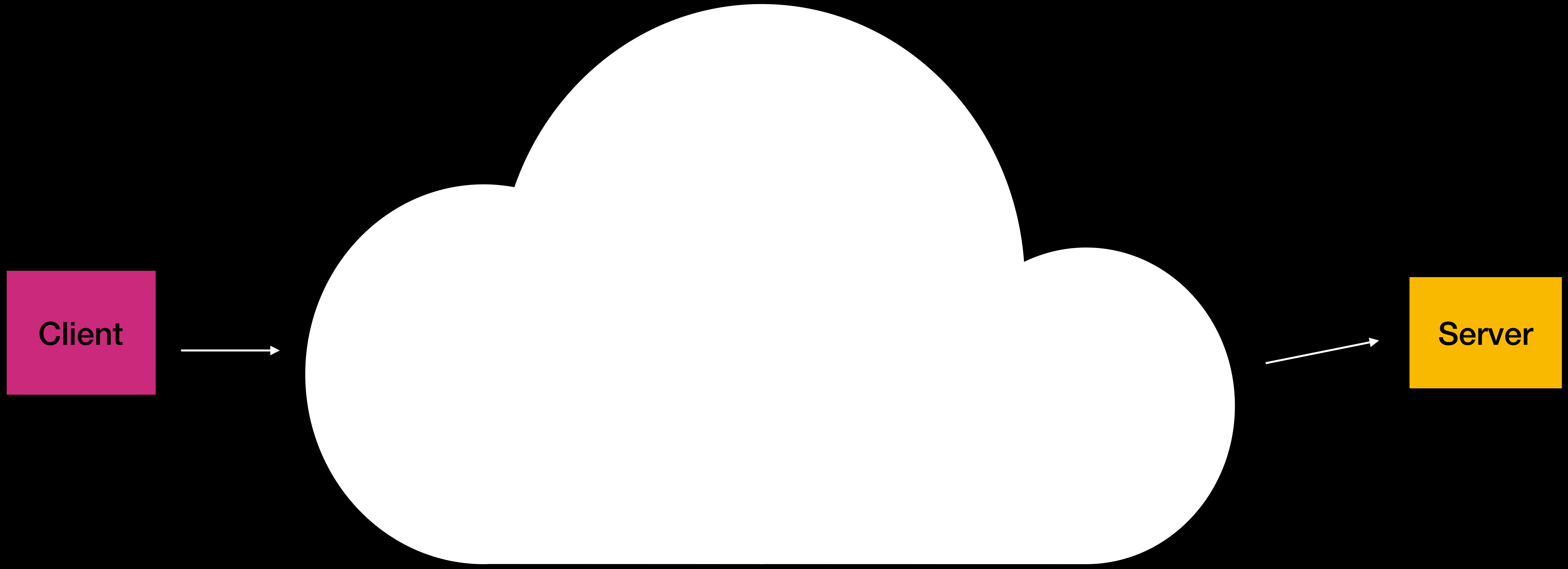


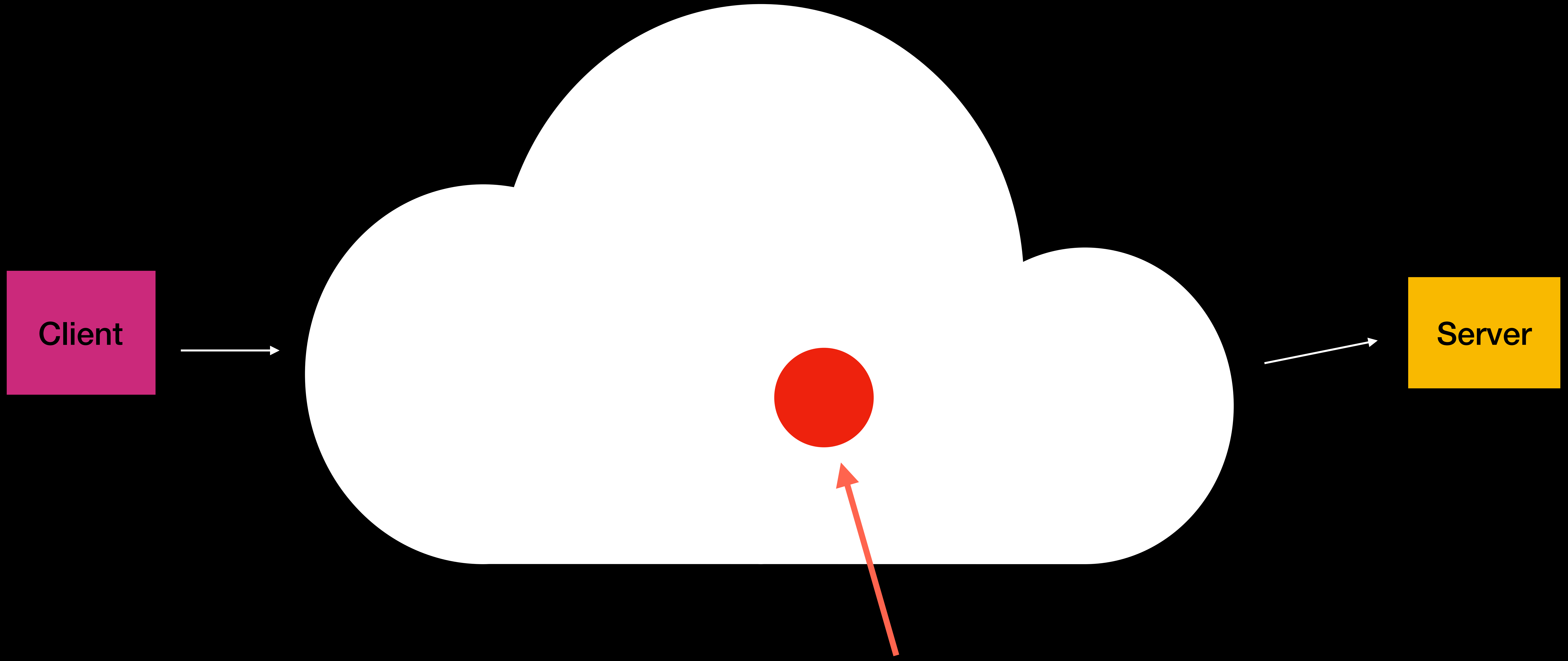




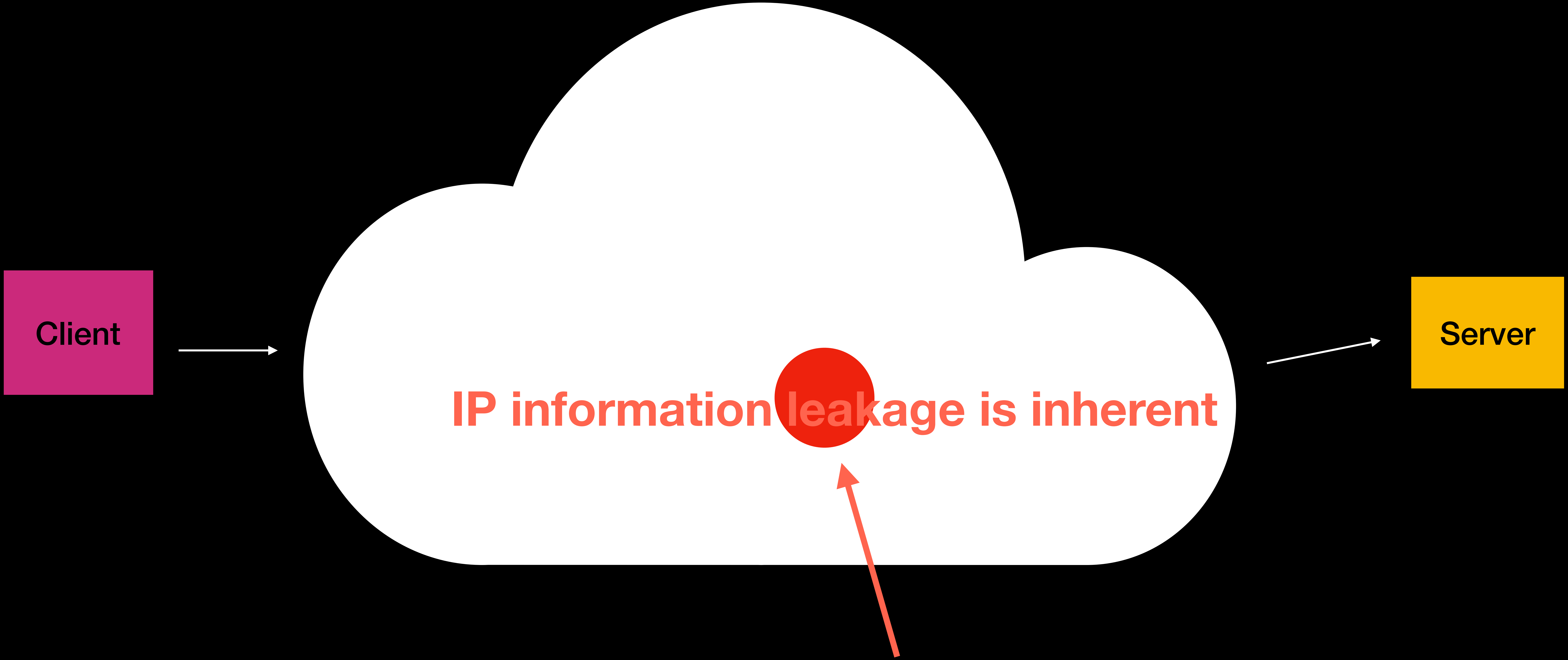
Client

Server


Client
Server



We know who its from and where it is going



Client

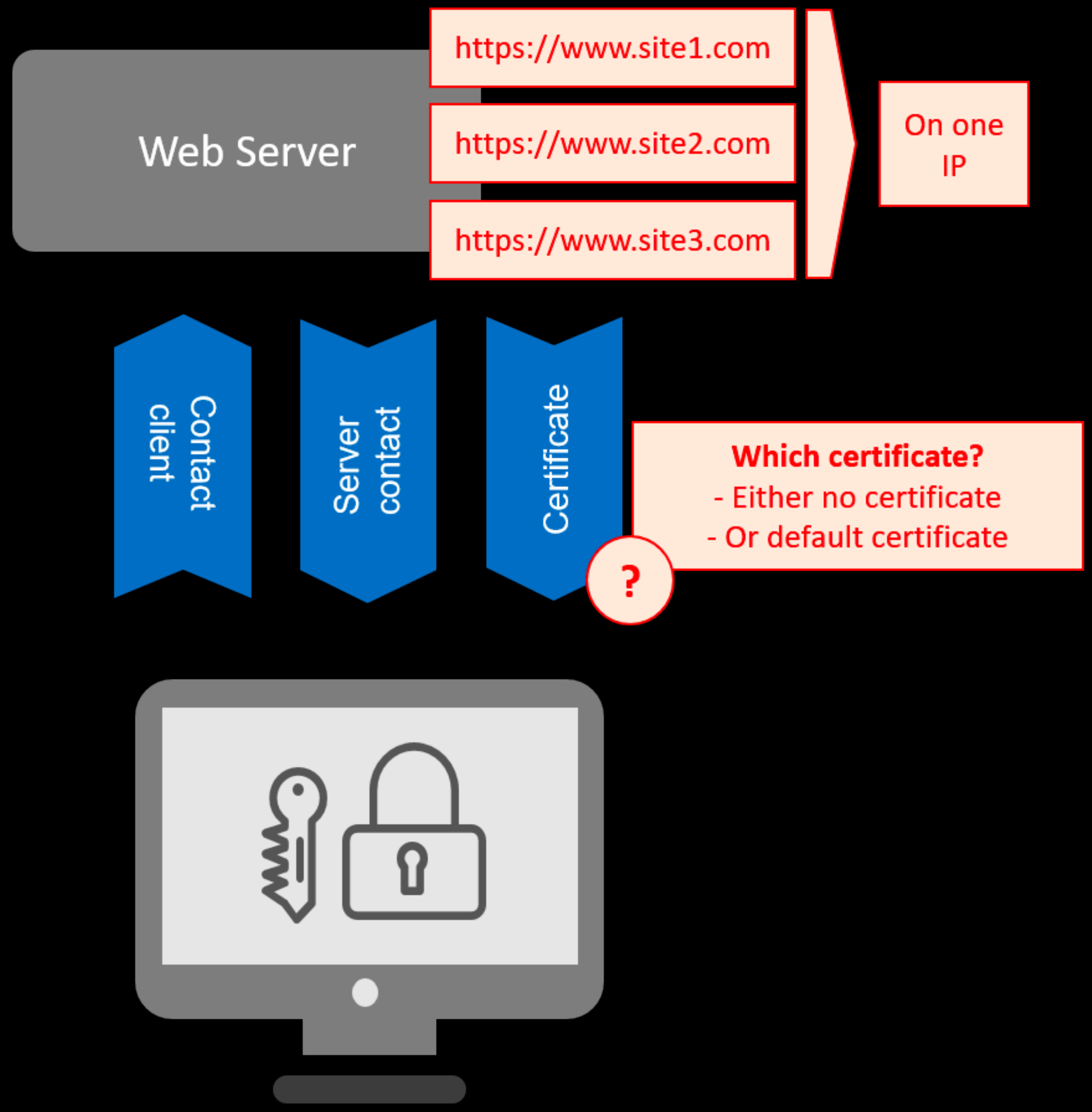
IP information leakage is inherent

Server

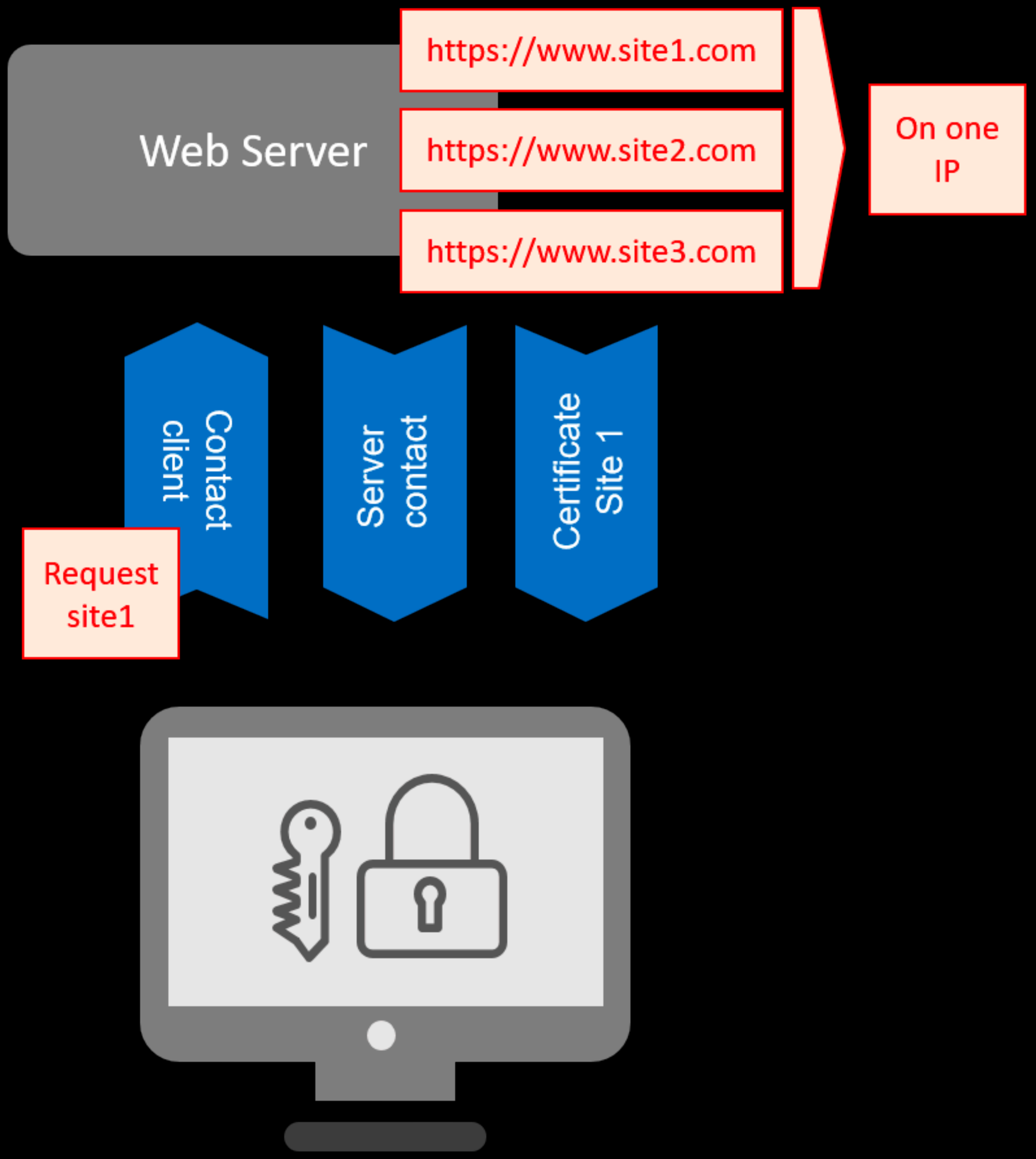
We know who its from and where it is going

IP information leakage is inherent

TLS Metadata - Server Name indication(SNI)



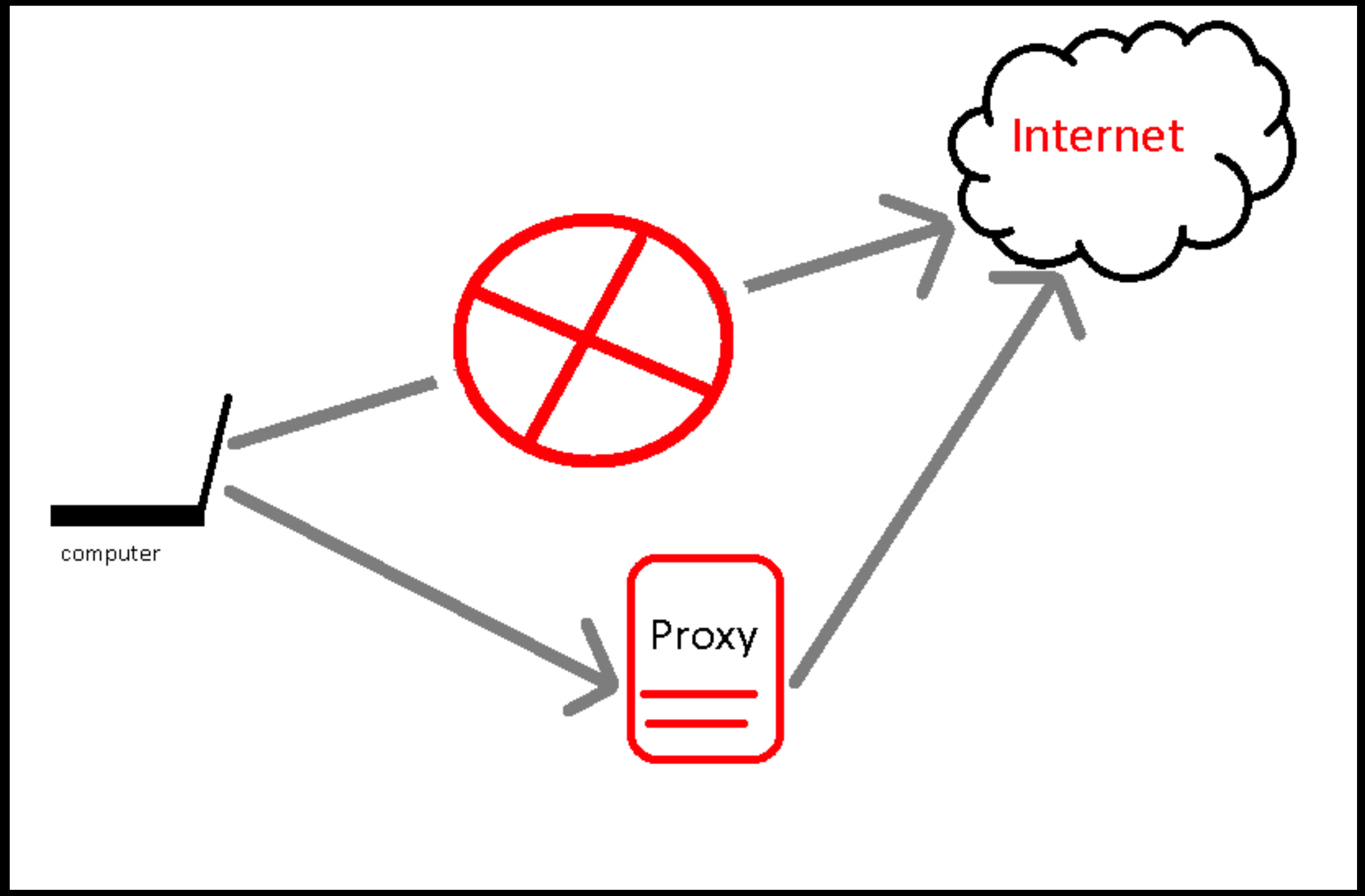
Which certificate?
- Either no certificate
- Or default certificate



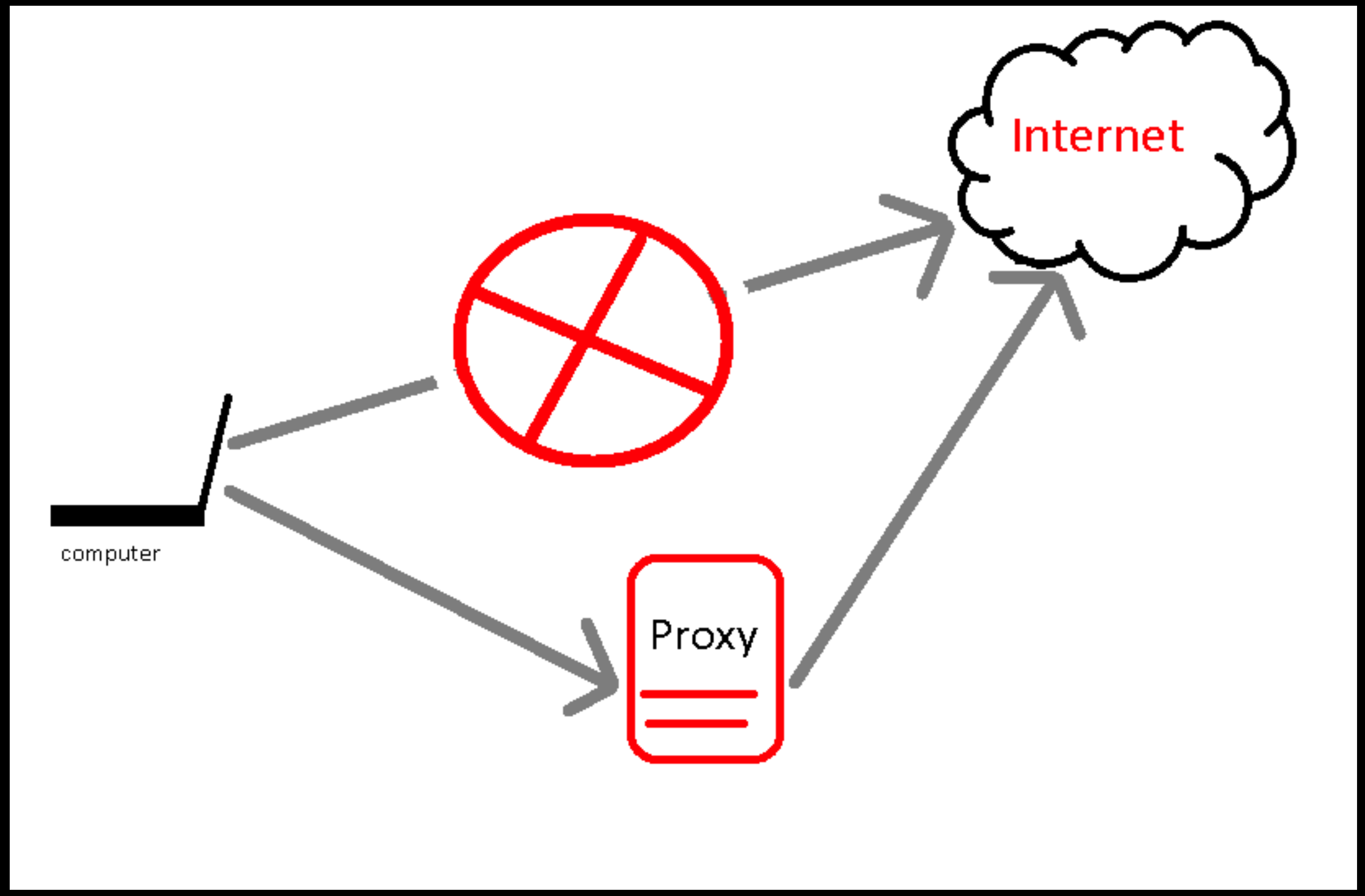
- Goal: Hide IP metadata when communicating over the internet

- Goal: Hide IP metadata when communicating over the internet
- Challenges:
  - Need IP for routing
  - IP Allows for selective blocking
- Solution?

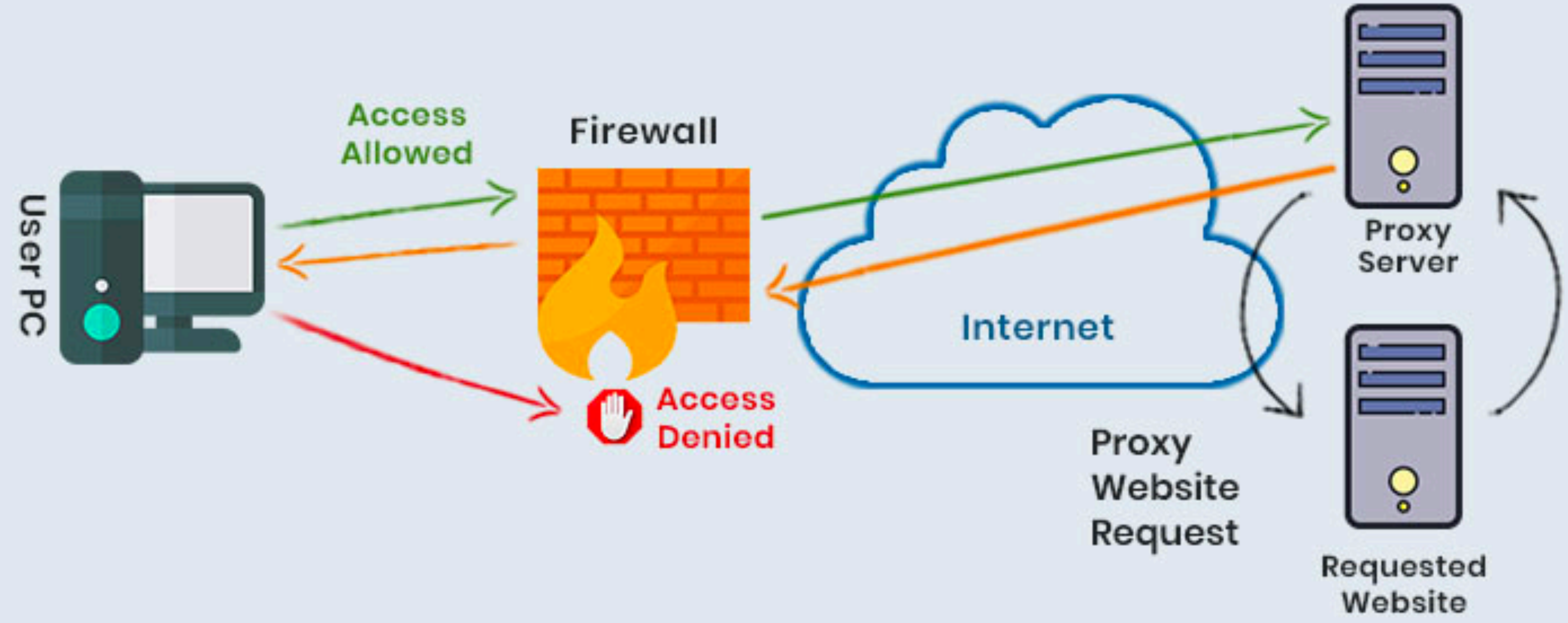
- Goal: Hide IP metadata when communicating over the internet
- Challenges:
  - Need IP for routing
  - IP Allows for selective blocking
- Solution?
  - VPN (Proxy)

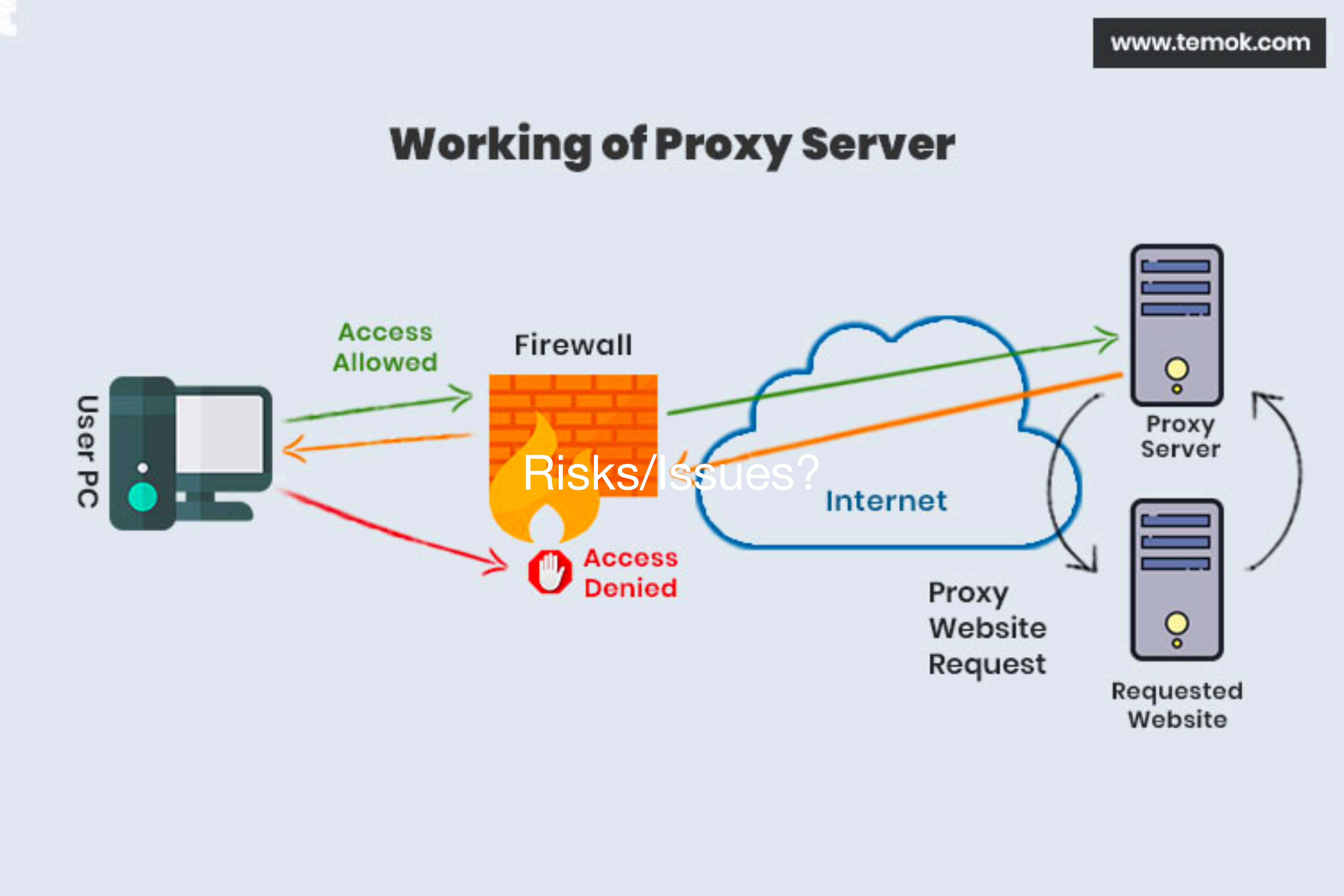


- Goal: Hide IP metadata when communicating over the internet
- Challenges:
  - Need IP for routing
  - IP Allows for selective blocking
- Solution?
  - VPN (Proxy)



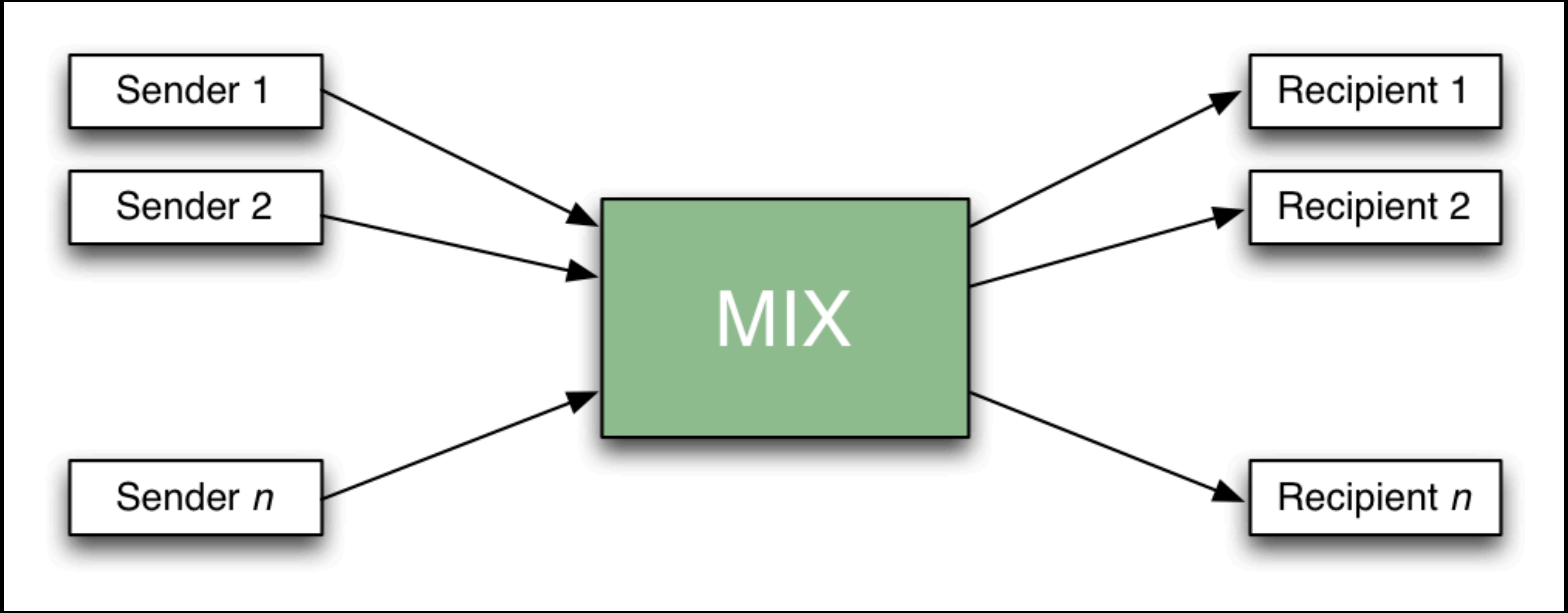
Working of Proxy Server

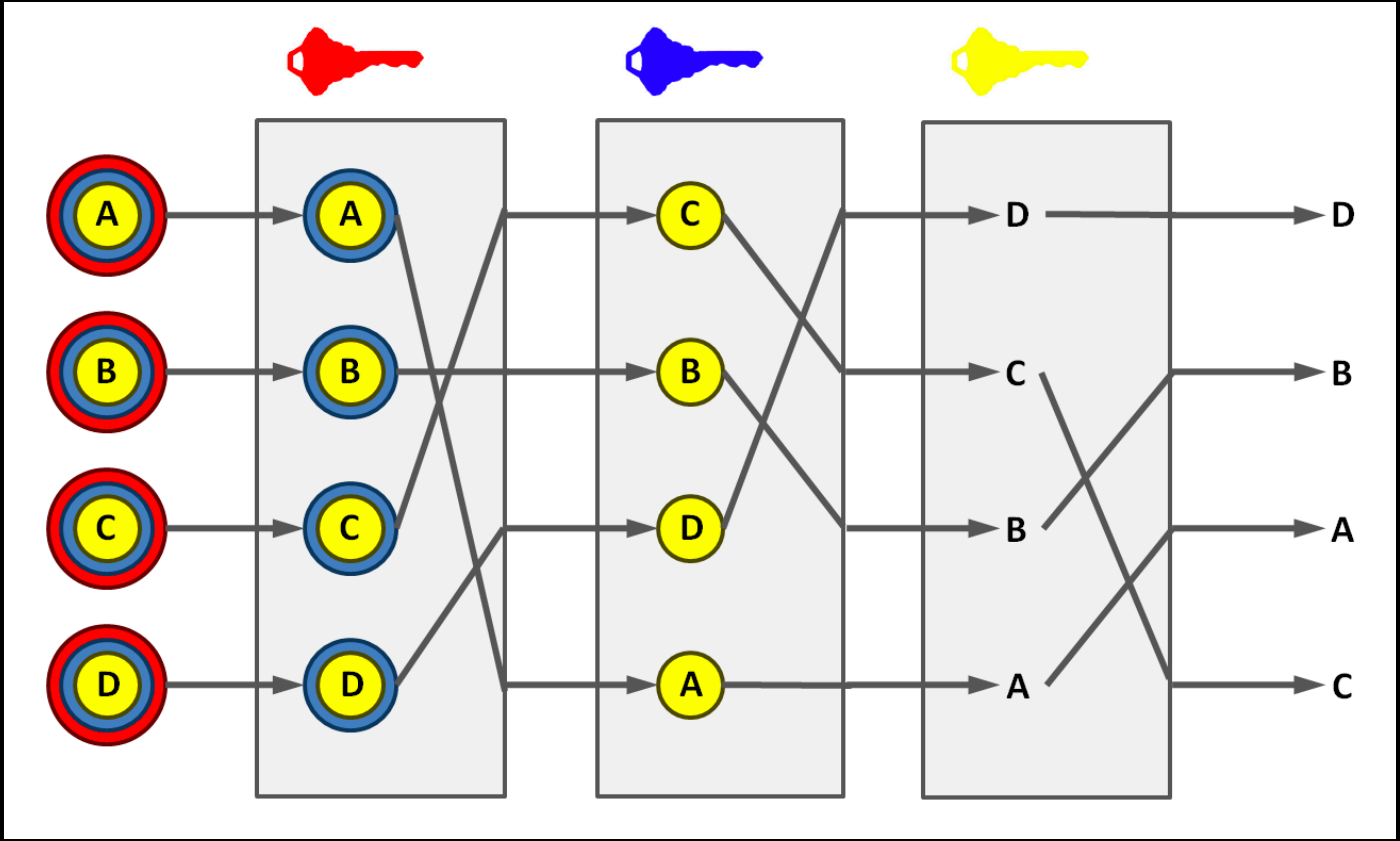


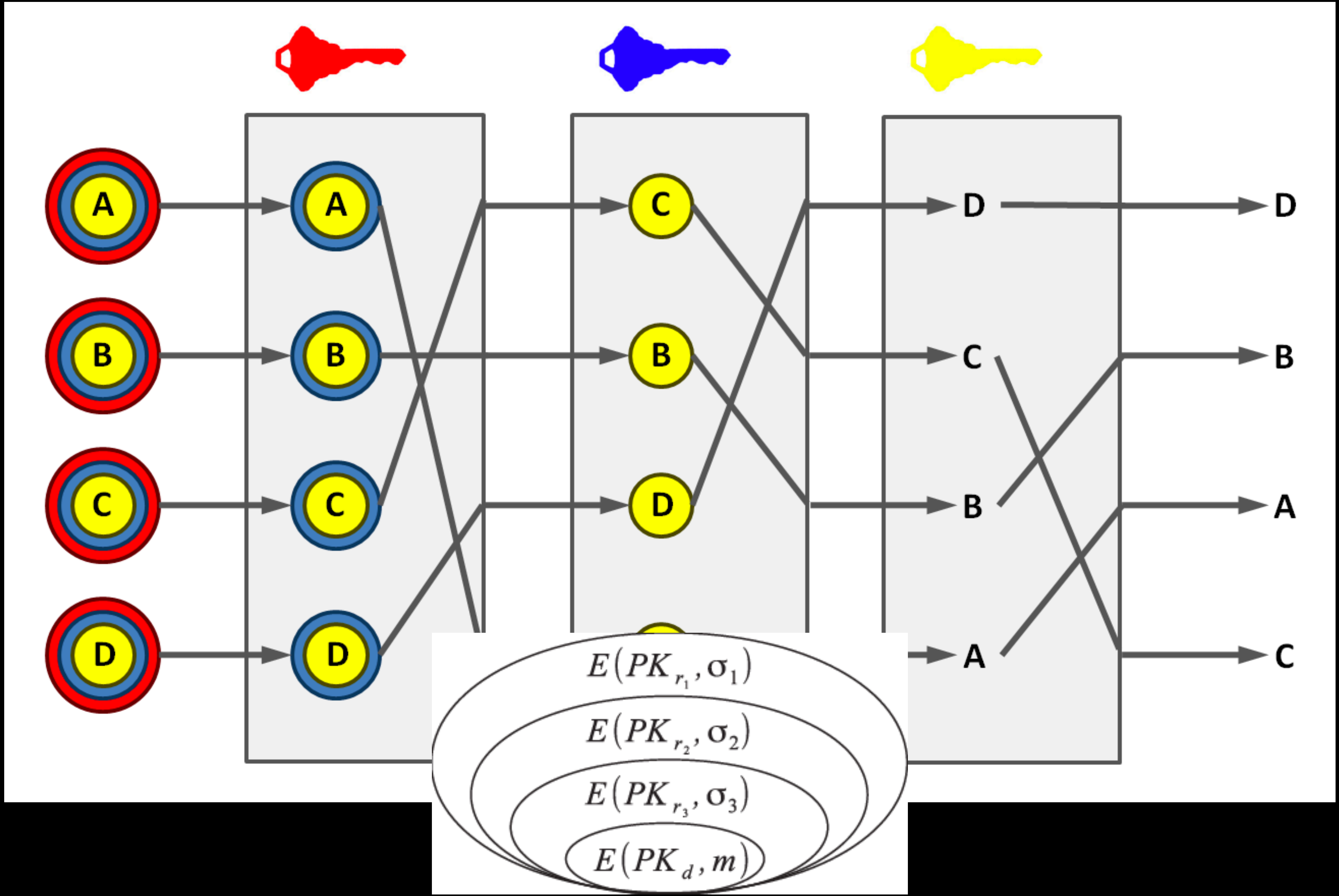


Risks/Issues?

Mix Nets

- 
Sender 1
Sender 2
Sender *n*
MIX
Recipient 1
Recipient 2
Recipient *n*


A
B
C
D
A
B
C
D
C
B
D
A
D
C
B
A
D
B
A
C



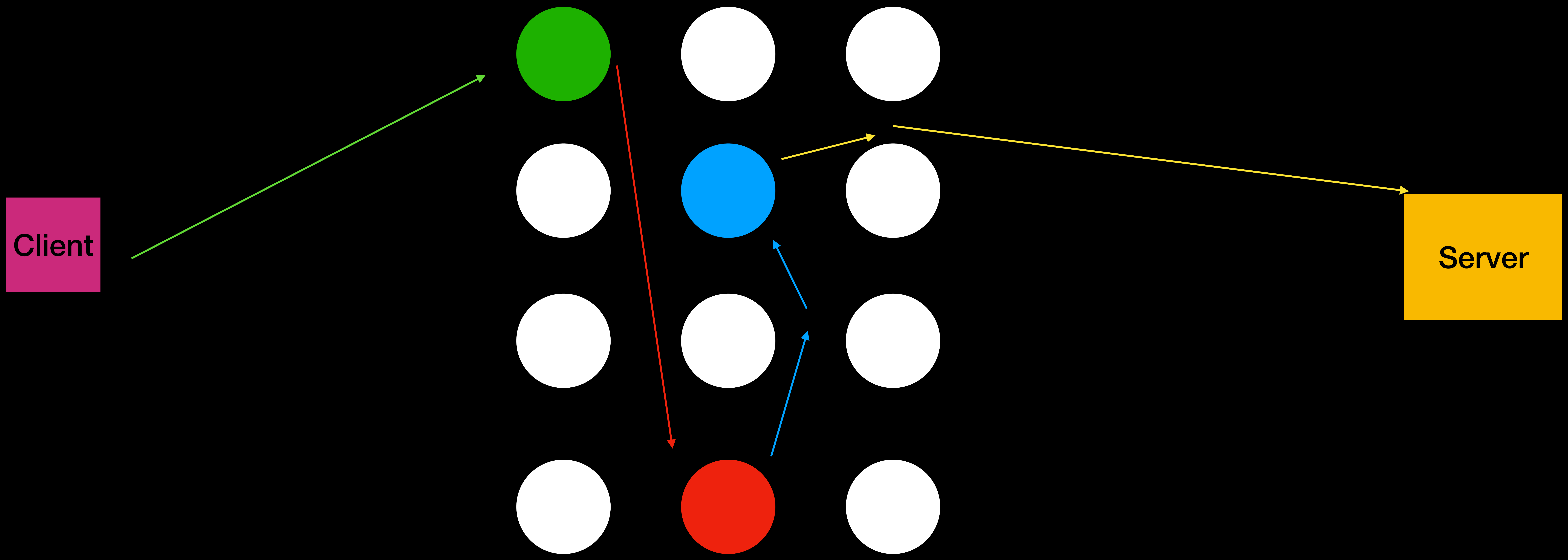
$E(PK_{r_1}, \sigma_1)$

$E(PK_{r_2}, \sigma_2)$

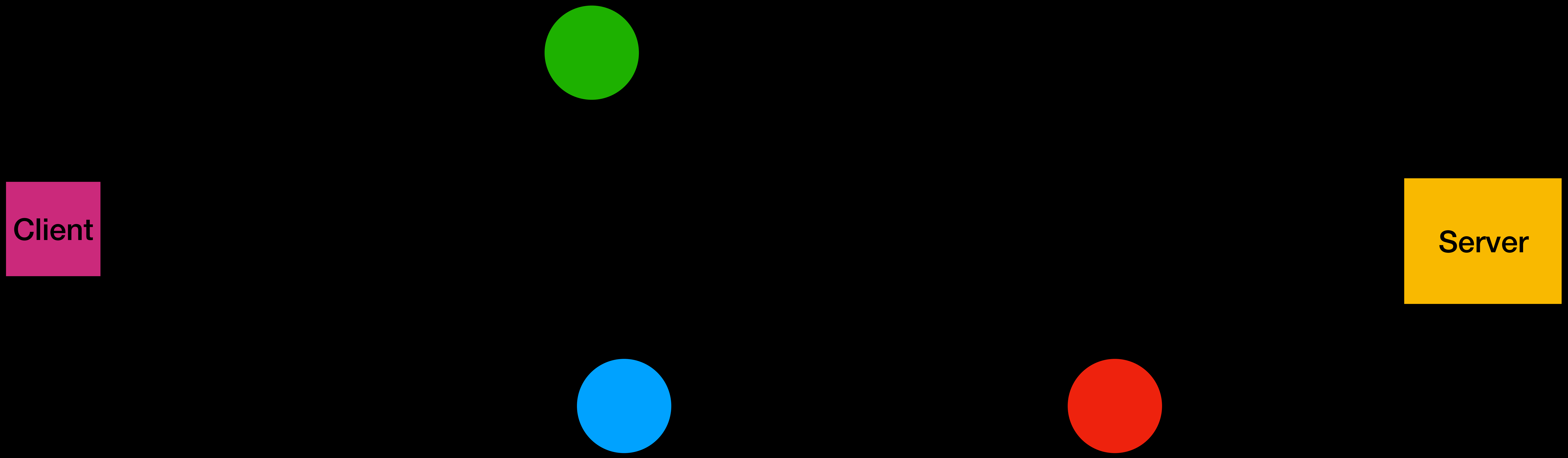
$E(PK_{r_3}, \sigma_3)$

$E(PK_d, m)$

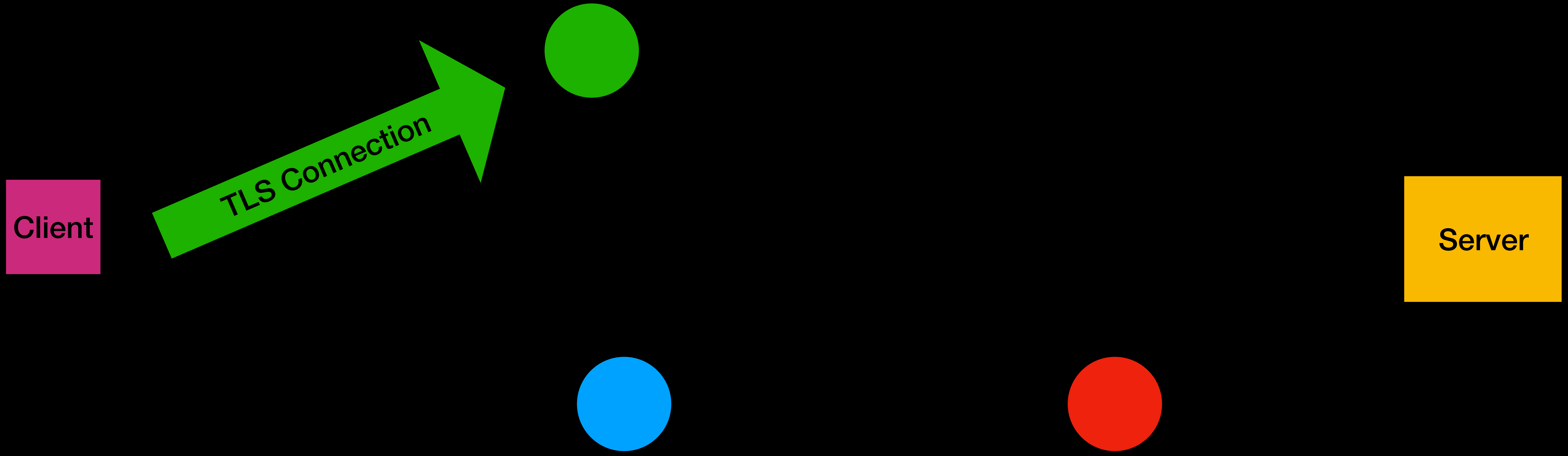
Tor as a mix net



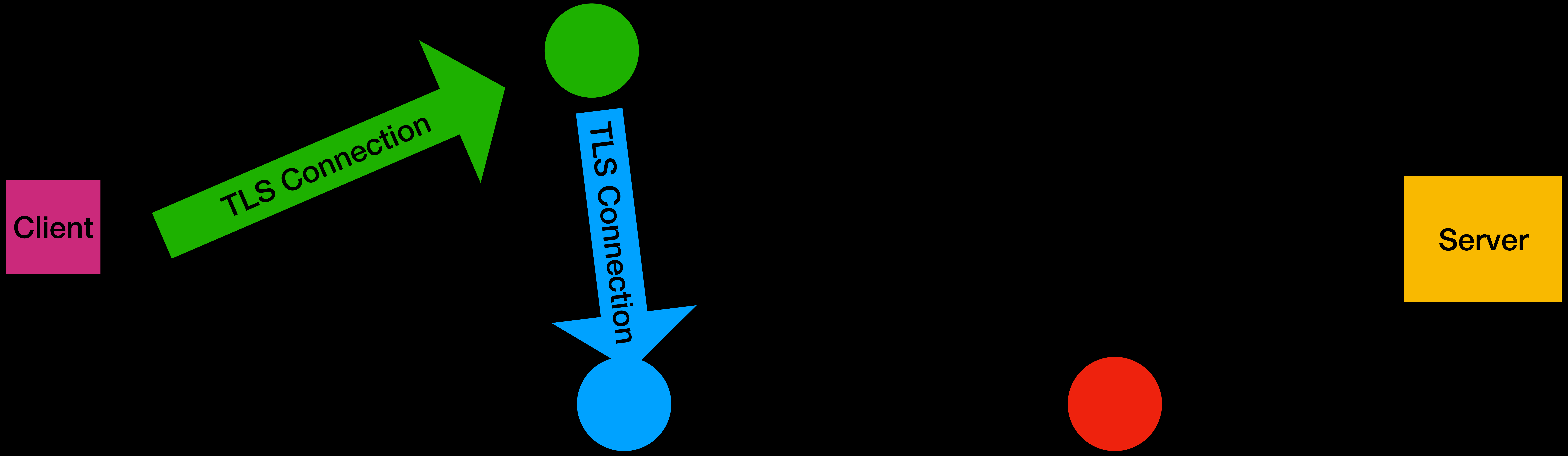
Tor Circuits



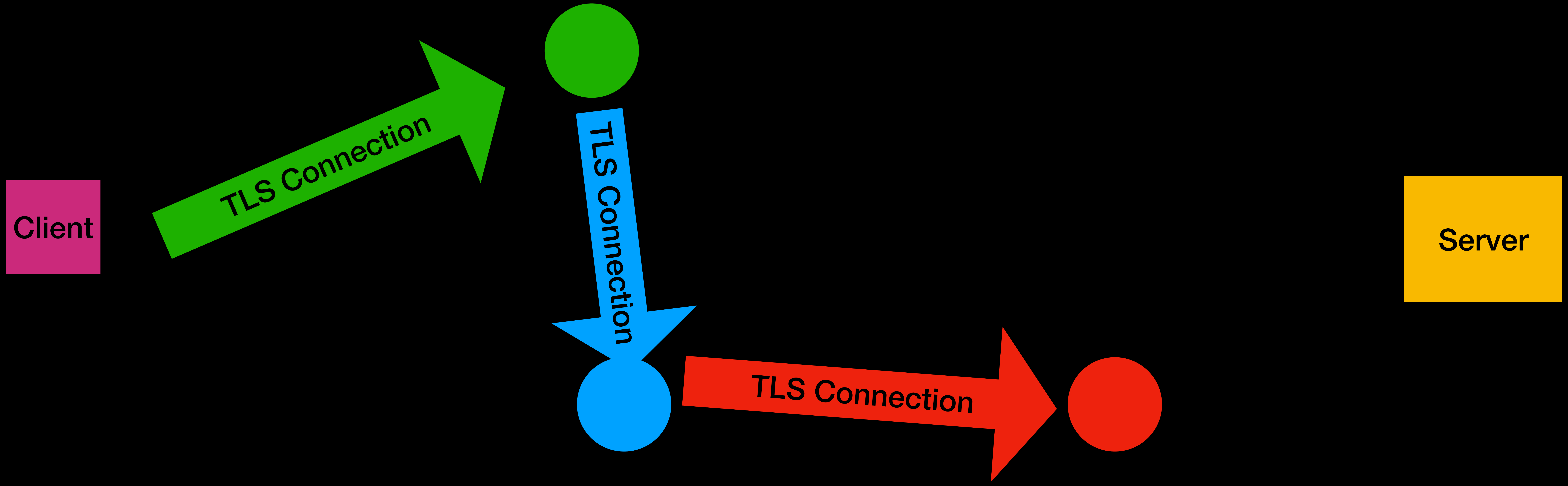
Tor Circuits



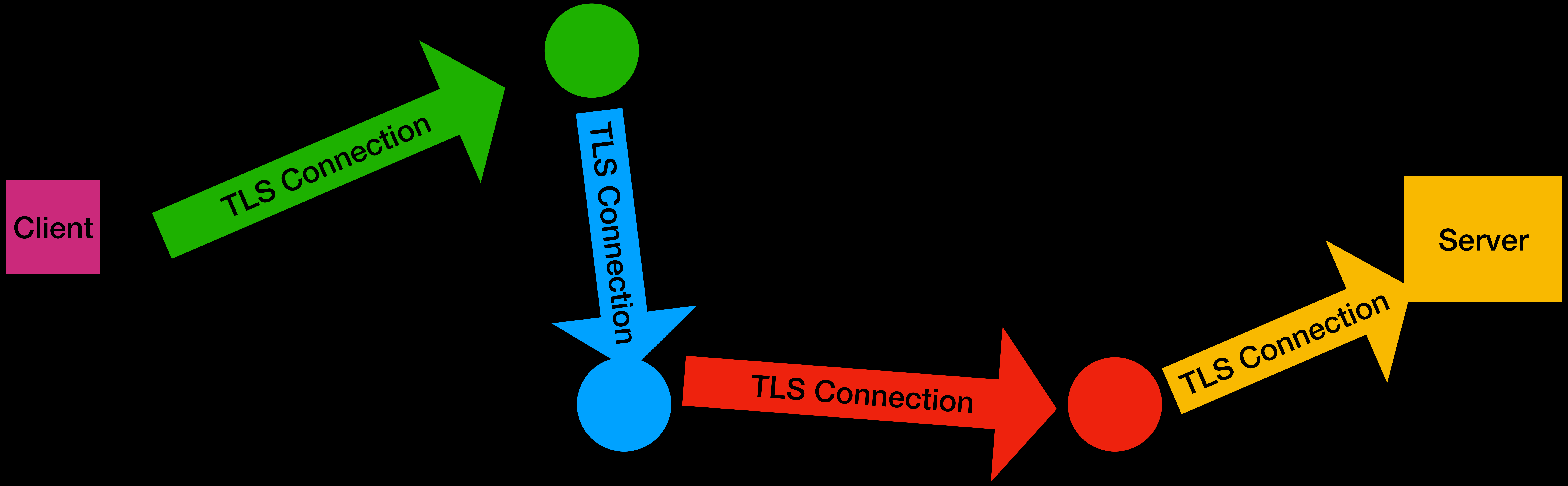
Tor Circuits

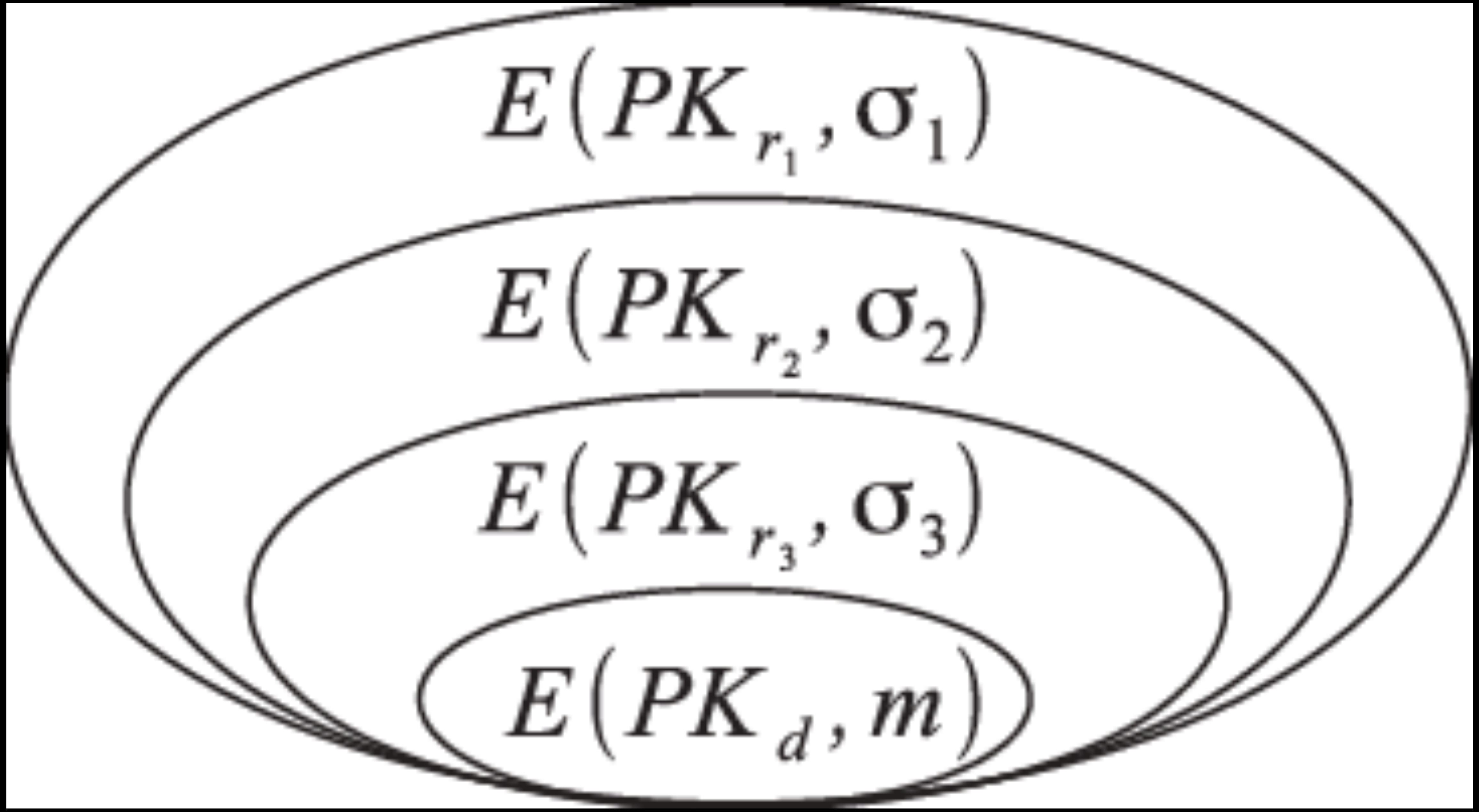


Tor Circuits

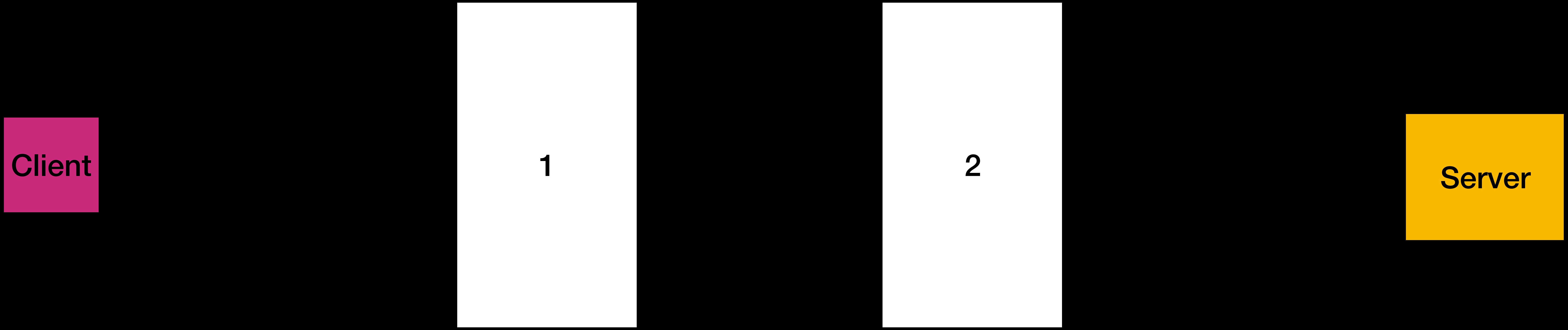


Tor Circuits




$E(PK_{r_1}, \sigma_1)$
$E(PK_{r_2}, \sigma_2)$
$E(PK_{r_3}, \sigma_3)$
$E(PK_d, m)$

Tor Circuit Creation



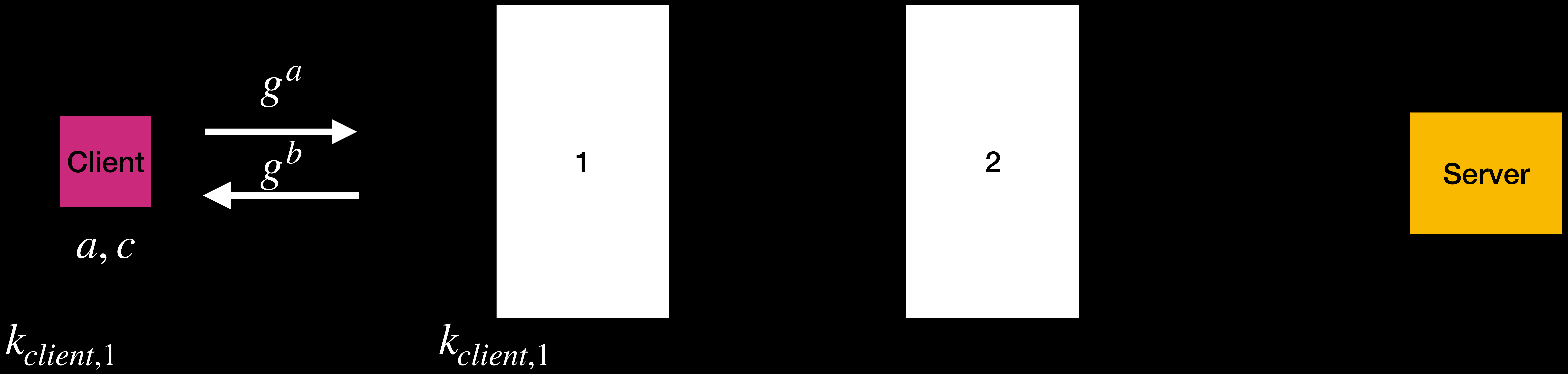
Client

1

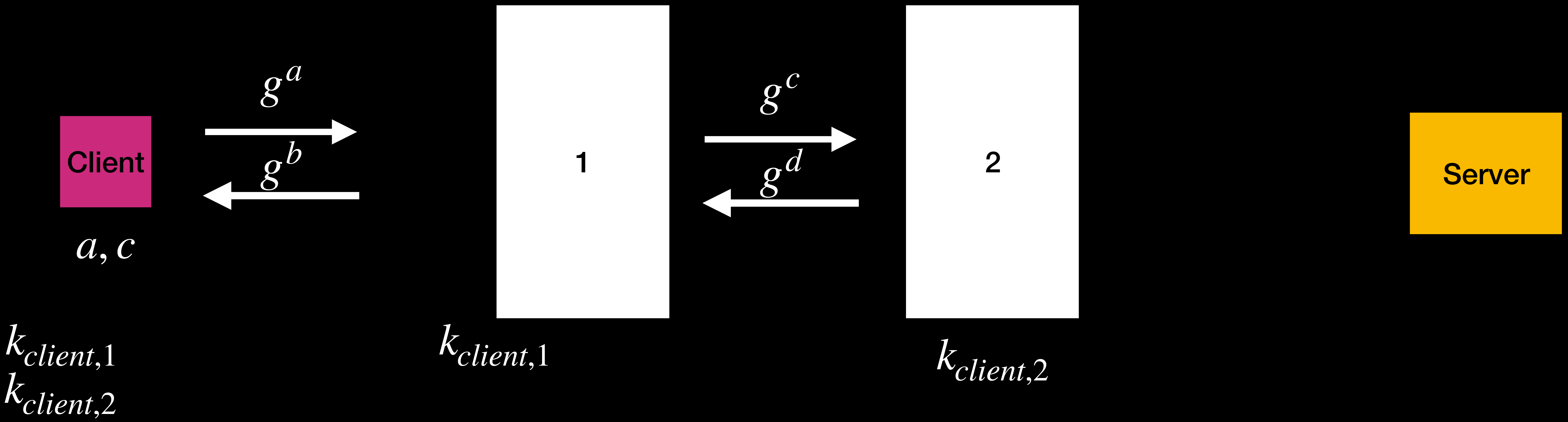
2

Server

Tor Circuit Creation



Tor Circuit Creation


Client
a, c
g^a
g^b
1
g^c
g^d
2
Server
$k_{client,1}$
$k_{client,2}$
$k_{client,1}$
$k_{client,2}$