An Analysis of the Tor Handshake

Akhil Kammila
Mentor: Kyle Hogan

Outline

1. Tor Introduction
2. Tor's Handshake
3. Improvements

1

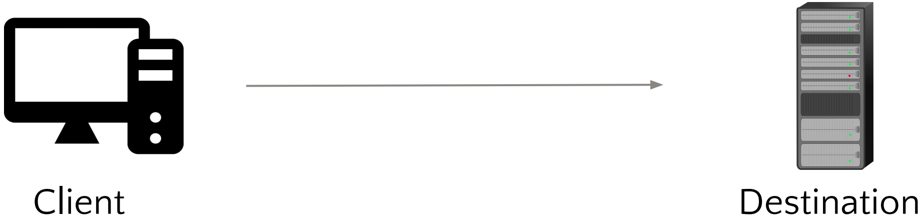
Tor Introduction

Anonymity

- Relationship anonymity

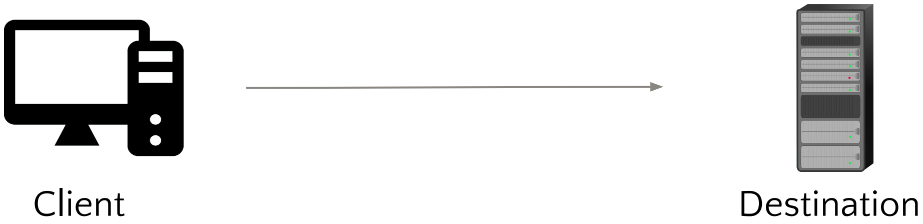
Anonymity

- Relationship anonymity



Anonymity

- Relationship anonymity

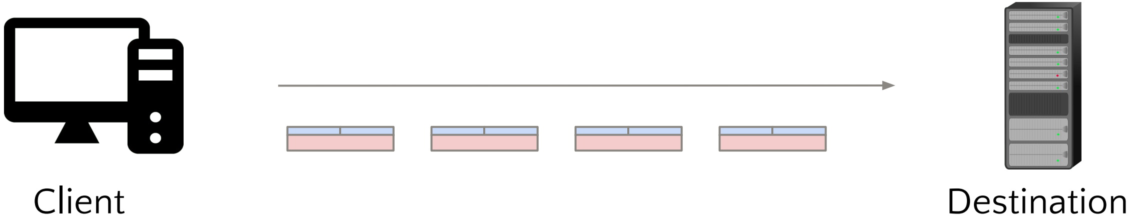


Client

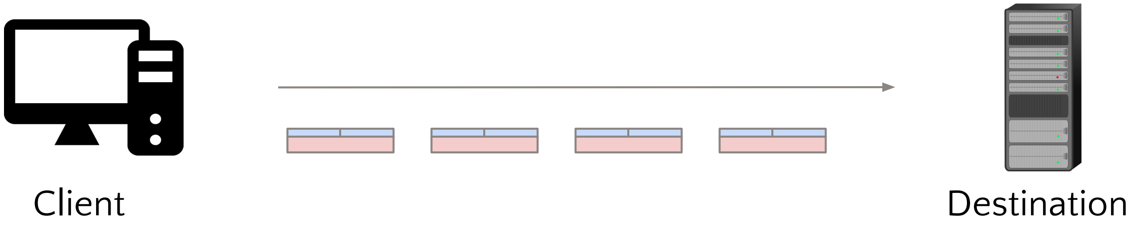
Destination

- Linkable

Normal Internet Connection

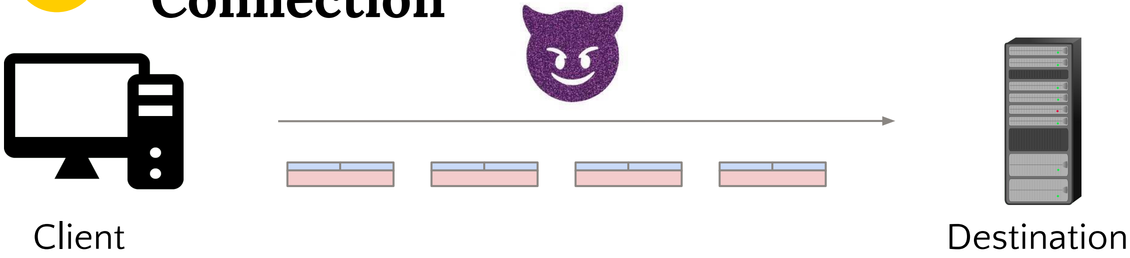


Normal Internet Connection



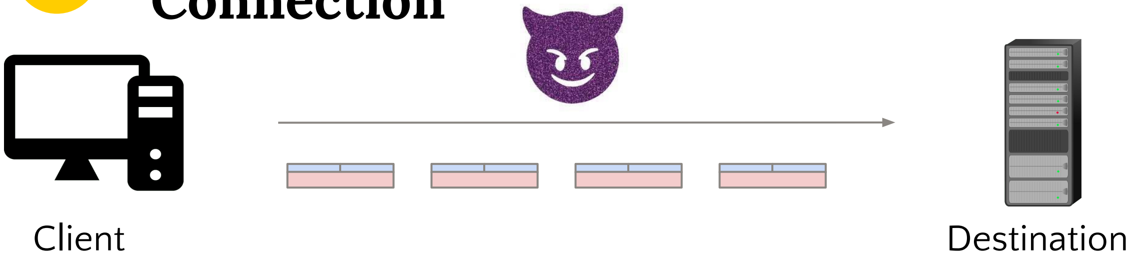
Source Address	Destination Address
Data 🔒	

Normal Internet Connection



Source Address	Destination Address
Data 🔒	

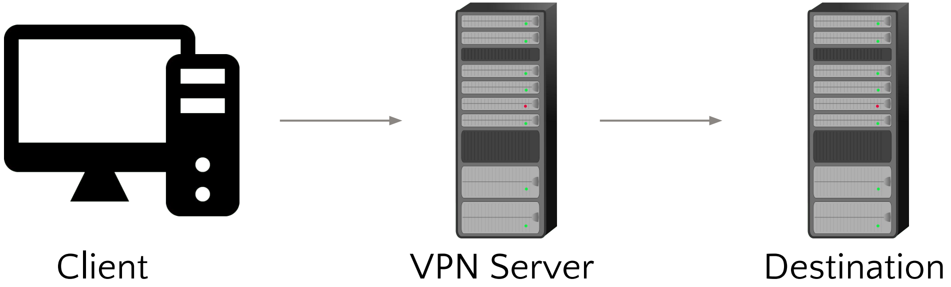
Normal Internet Connection



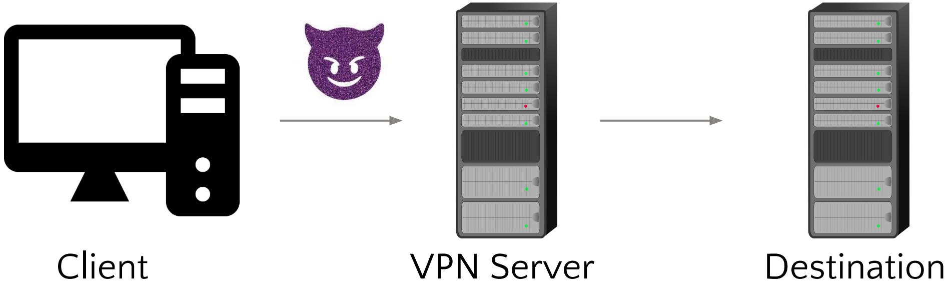
Source Address	Destination Address
Data 🔒	

– Linkable by anyone viewing the connection ✗

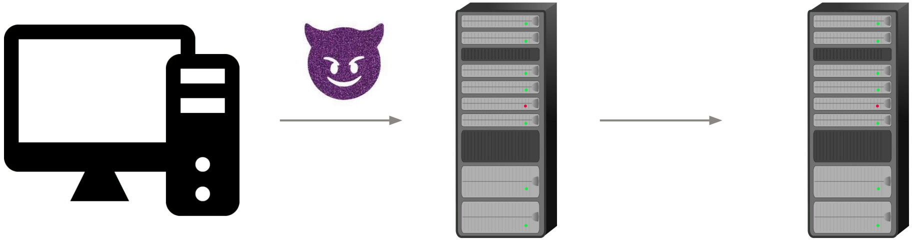
VPN Connection



VPN Connection



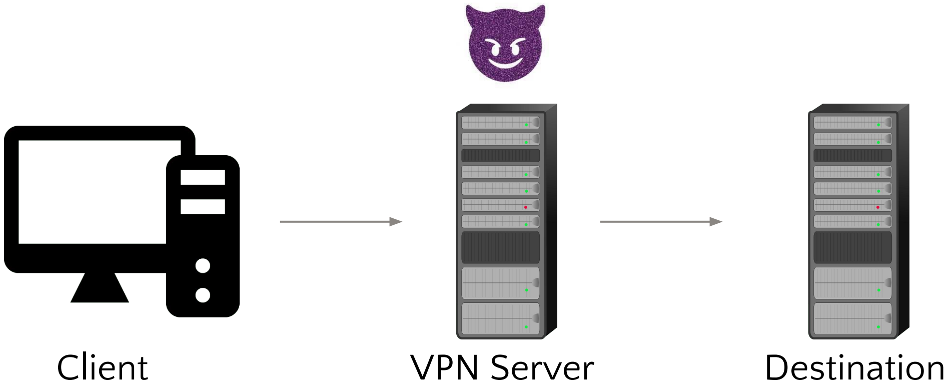
VPN Connection



Client VPN Server Destination

– Not linkable by anyone viewing the connection ✓

VPN Connection



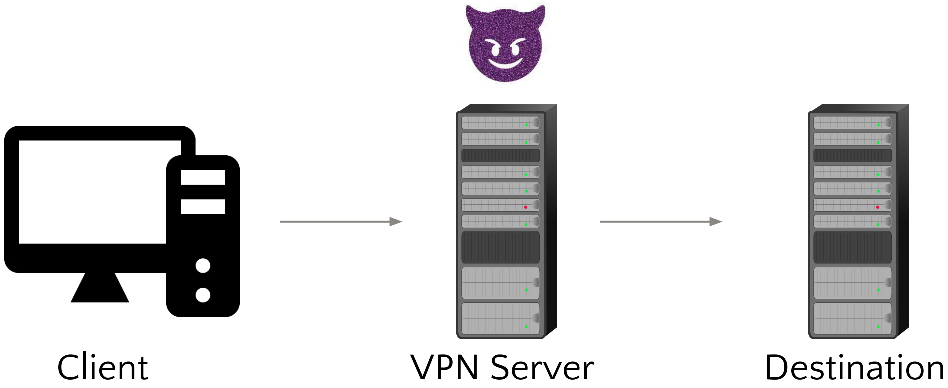
Client

VPN Server

Destination

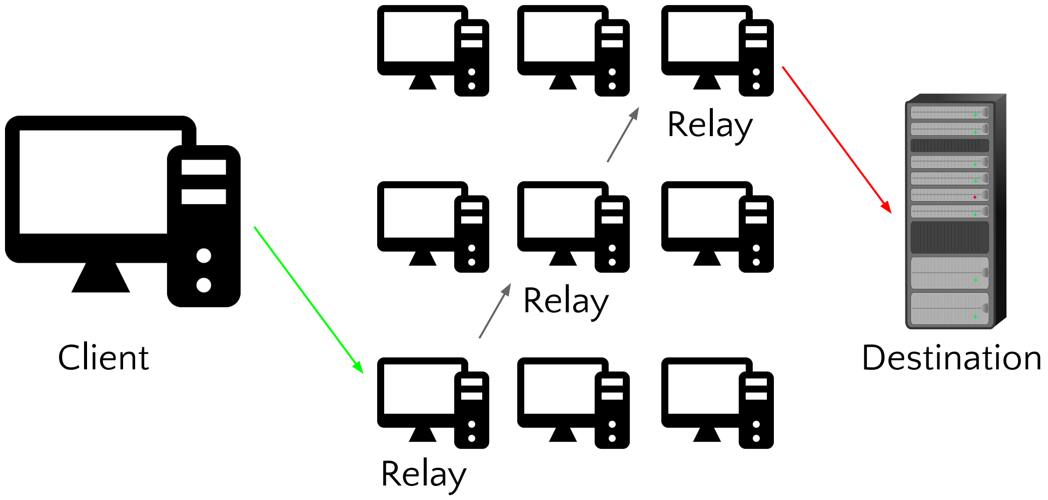
– Not linkable by anyone viewing the connection ✓

VPN Connection

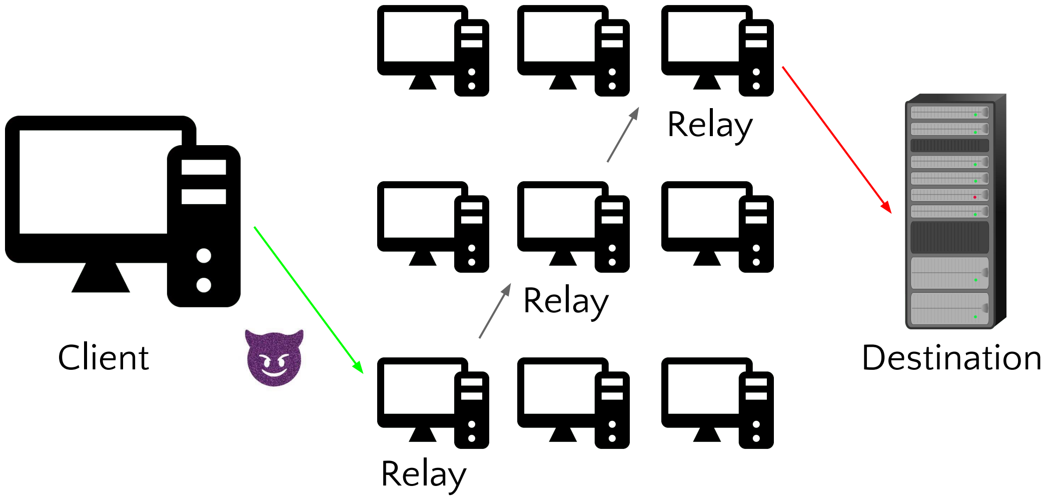


- Not linkable by anyone viewing the connection ✓
- Linkable by the VPN server ✗

Tor Internet Connection

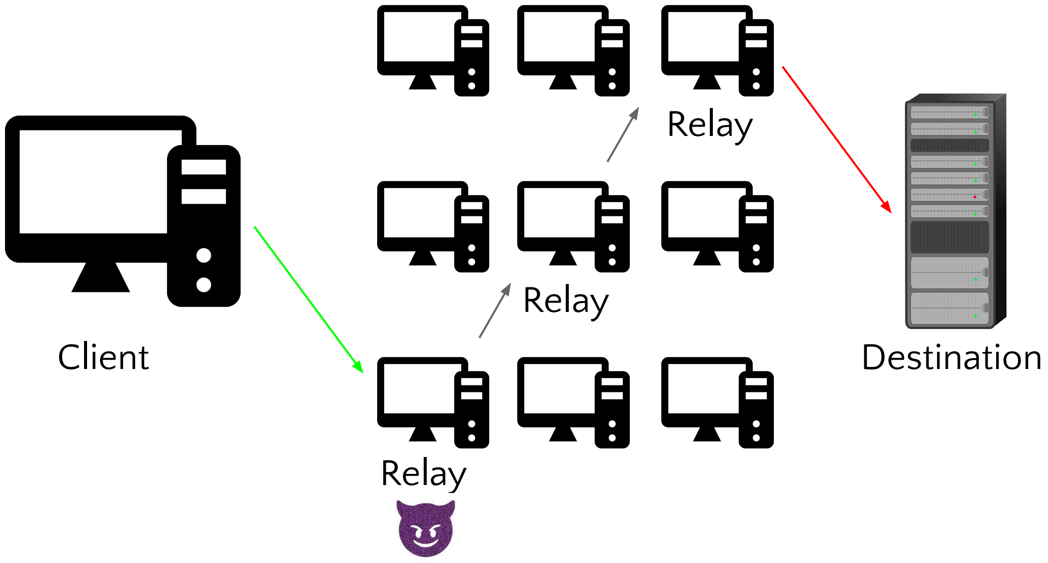


Tor Internet Connection



– Not linkable by anyone viewing the connection ✓

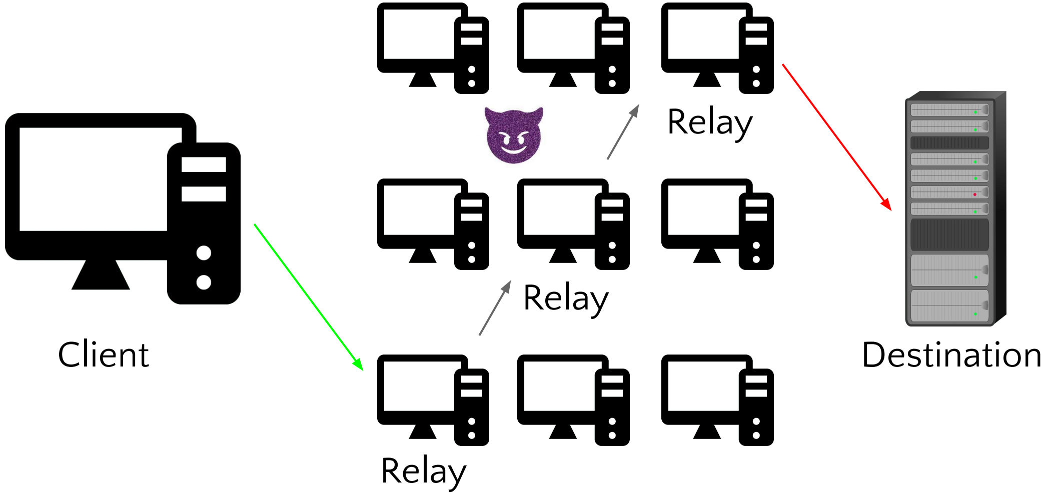
Tor Internet Connection



- Not linkable by anyone viewing the connection ✓

- Not linkable by relays ✓

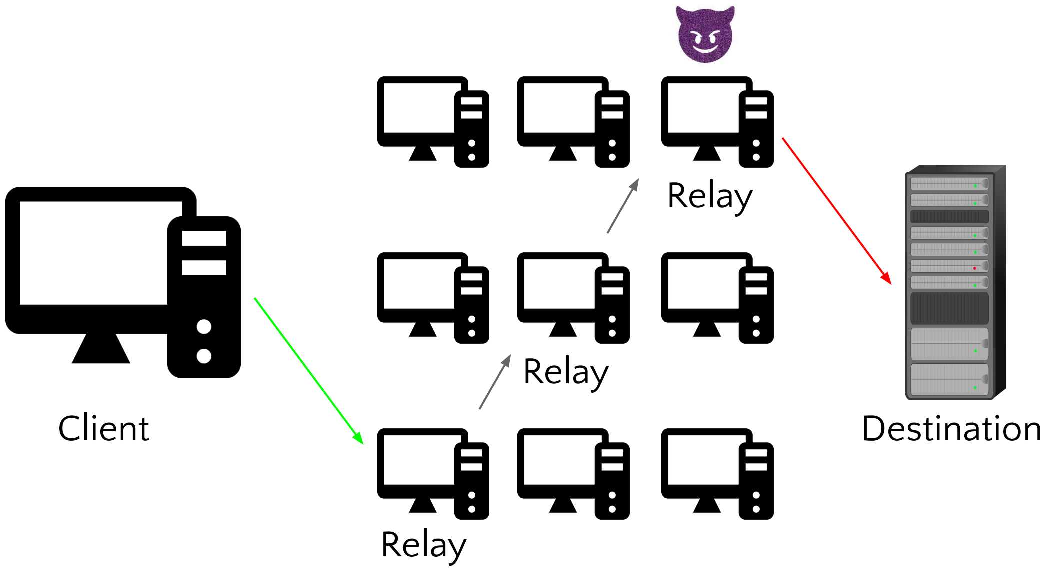
Tor Internet Connection



- Not linkable by anyone viewing the connection ✓

- Not linkable by relays ✓

Tor Internet Connection



- Not linkable by anyone viewing the connection ✓

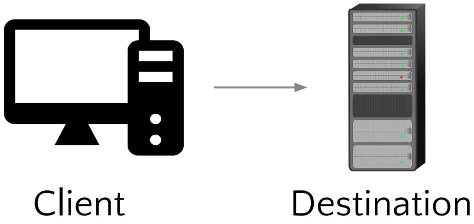
- Not linkable by relays ✓

2

Tor’s Handshake

Why Handshake?

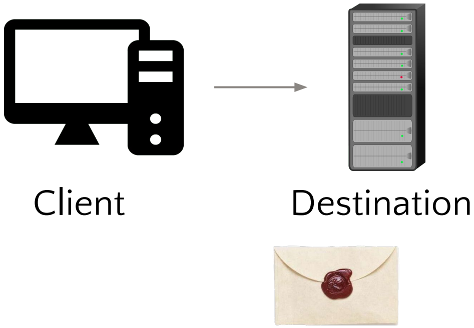
Normal connection



1. Authentication

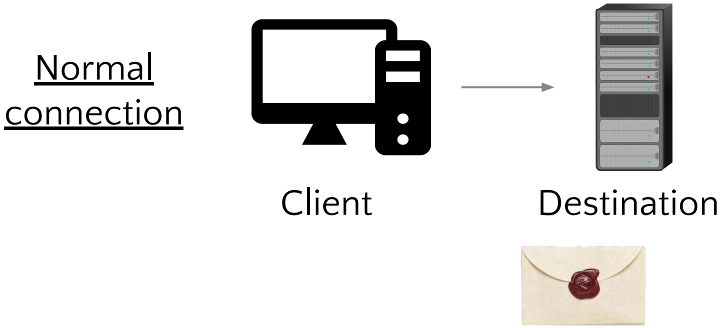
Why Handshake?

Normal connection

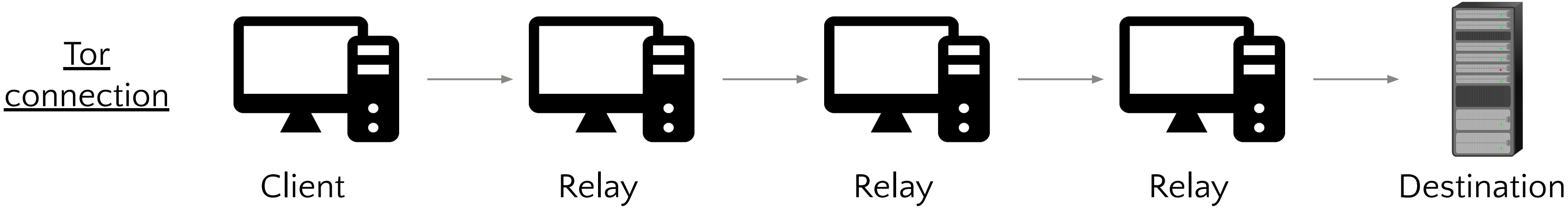


1. Authentication

Why Handshake?

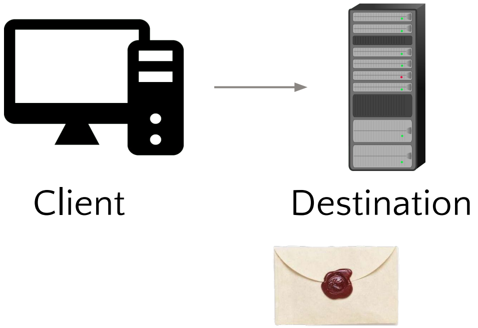


1. Authentication

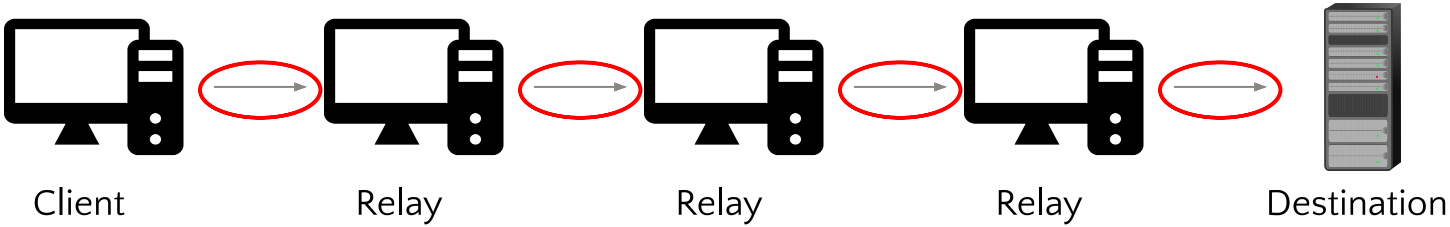


Why Handshake?

Normal connection

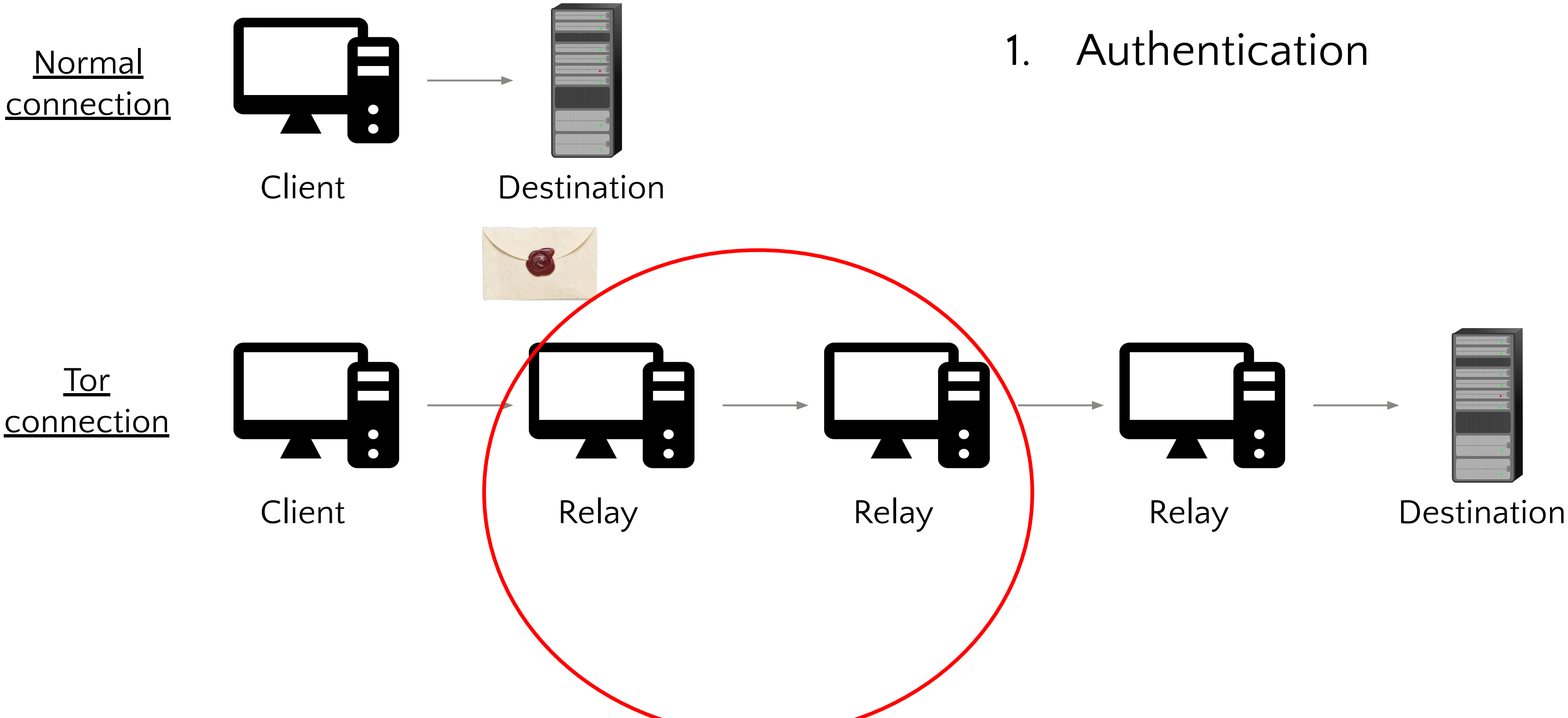


Tor connection



1. Authentication

Why Handshake?



Normal connection

Client

Destination

Tor connection

Client

Relay

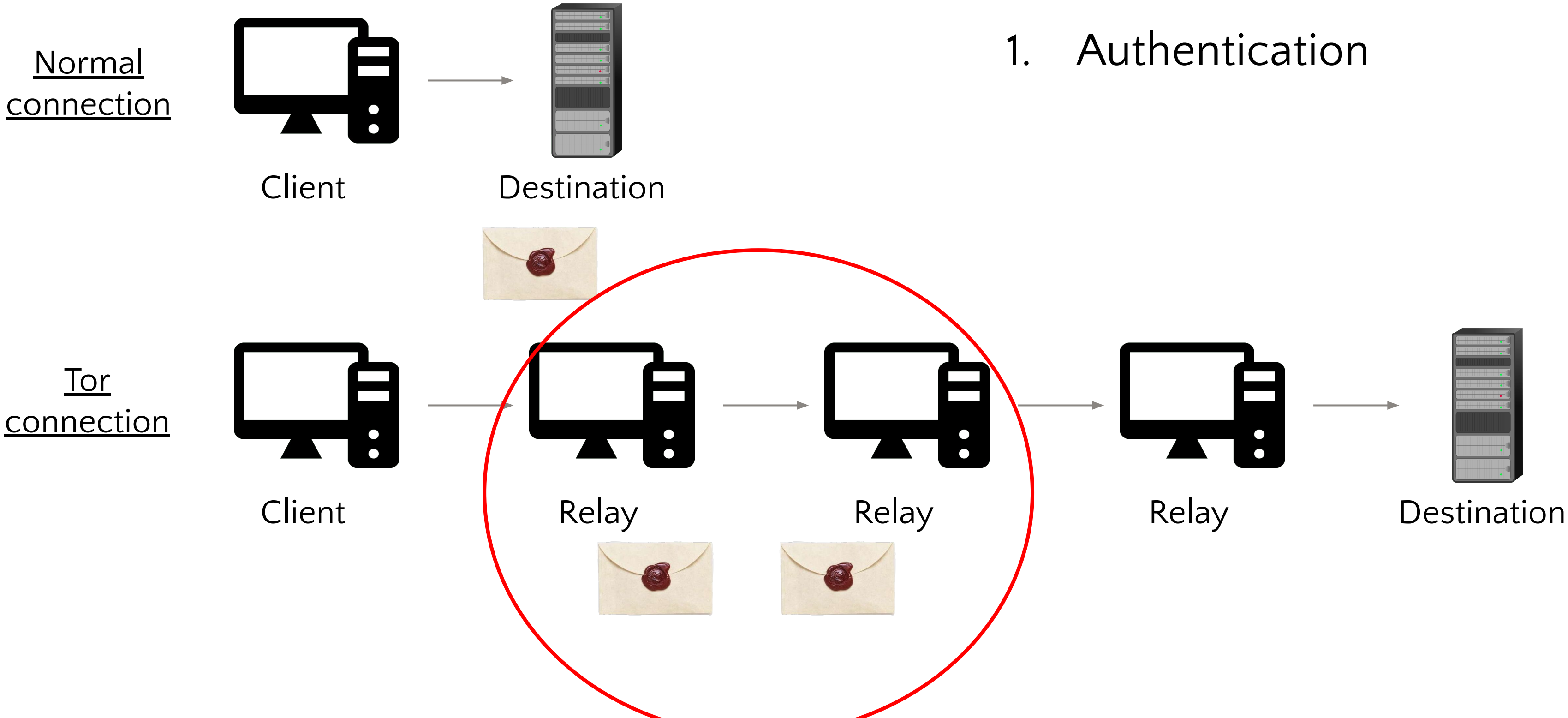
Relay

Relay

Destination

1. Authentication

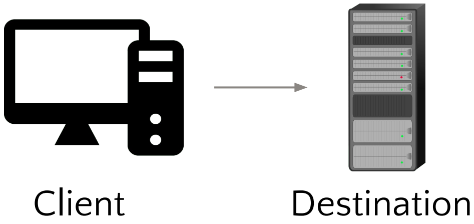
Why Handshake?



1. Authentication

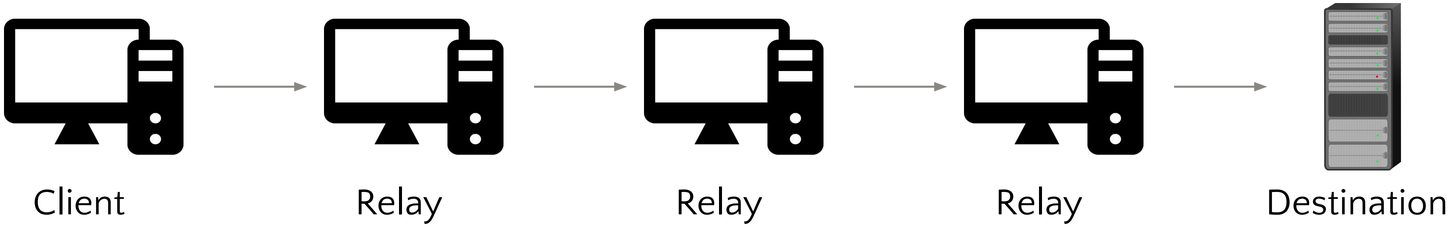
Why Handshake?

Normal connection

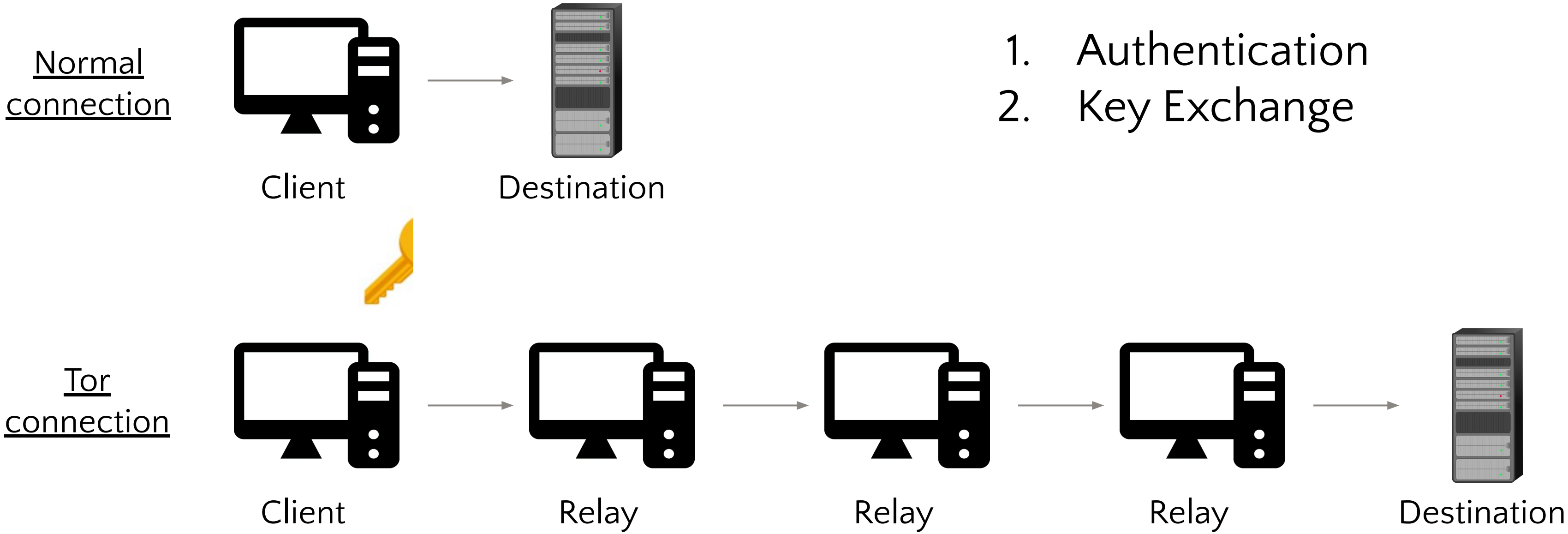


1. Authentication
2. Key Exchange

Tor connection



Why Handshake?



Normal connection

Client

Destination

Tor connection

Client

Relay

Relay

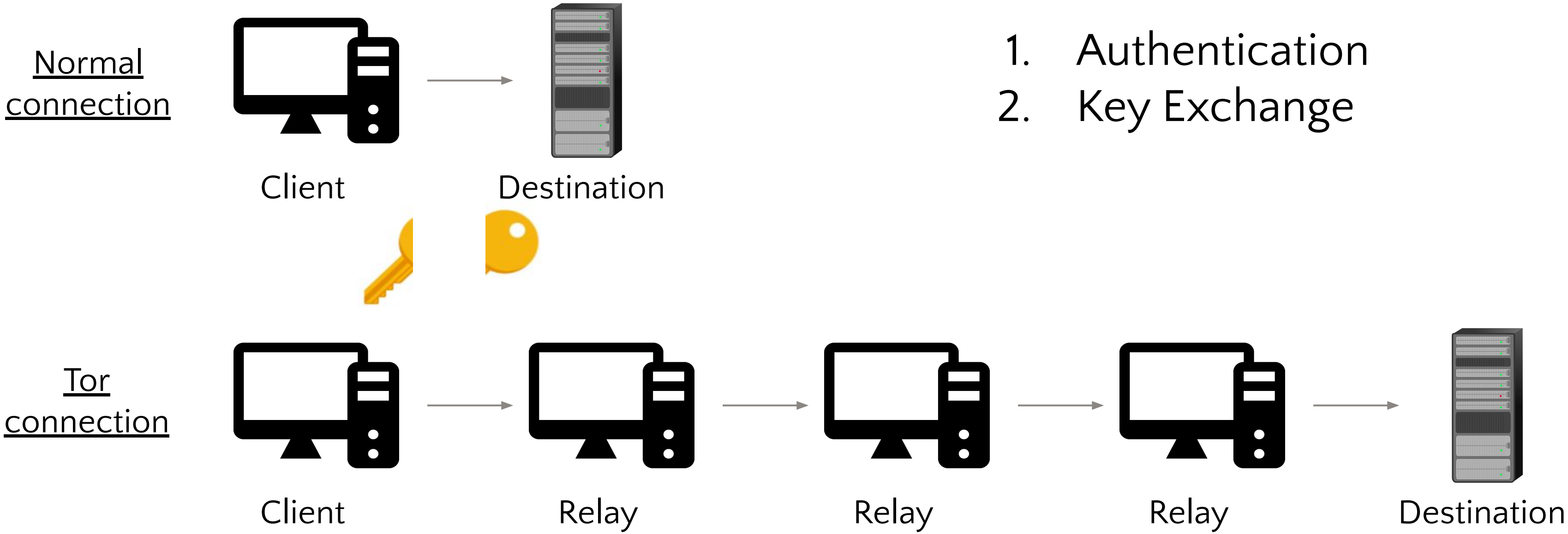
Relay

Destination

1. Authentication
2. Key Exchange

Why Handshake?

1. Authentication
2. Key Exchange



Normal connection

Client

Destination

Tor connection

Client

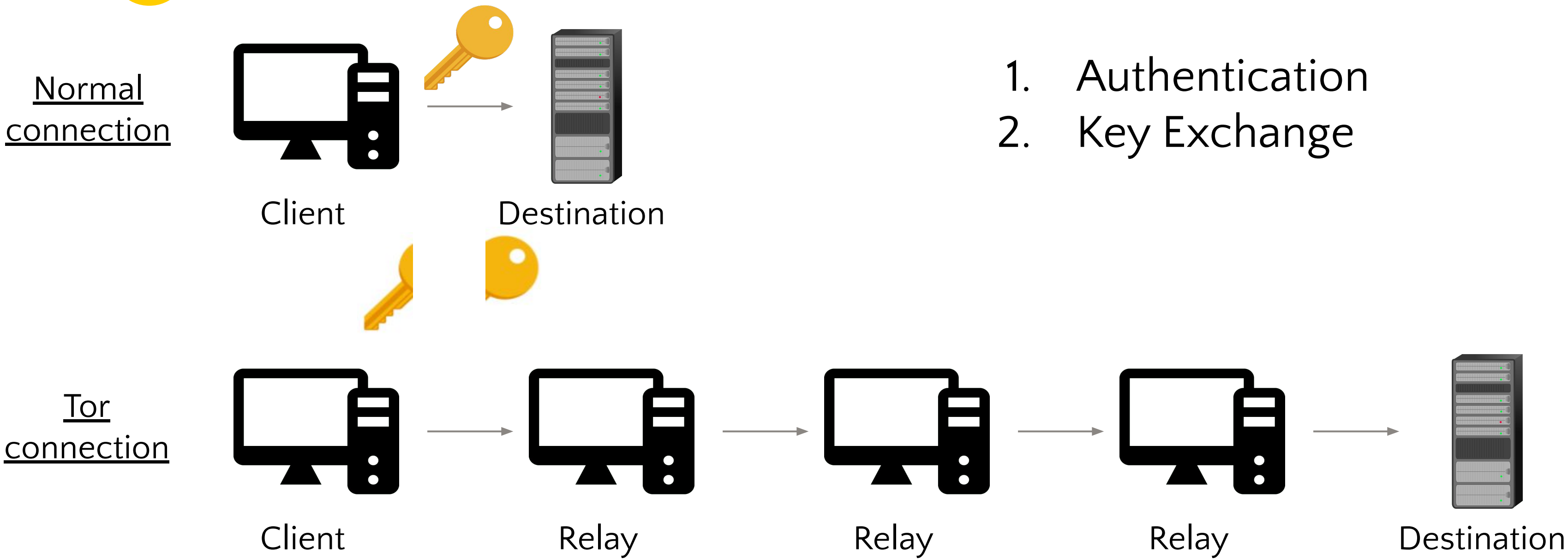
Relay

Relay

Relay

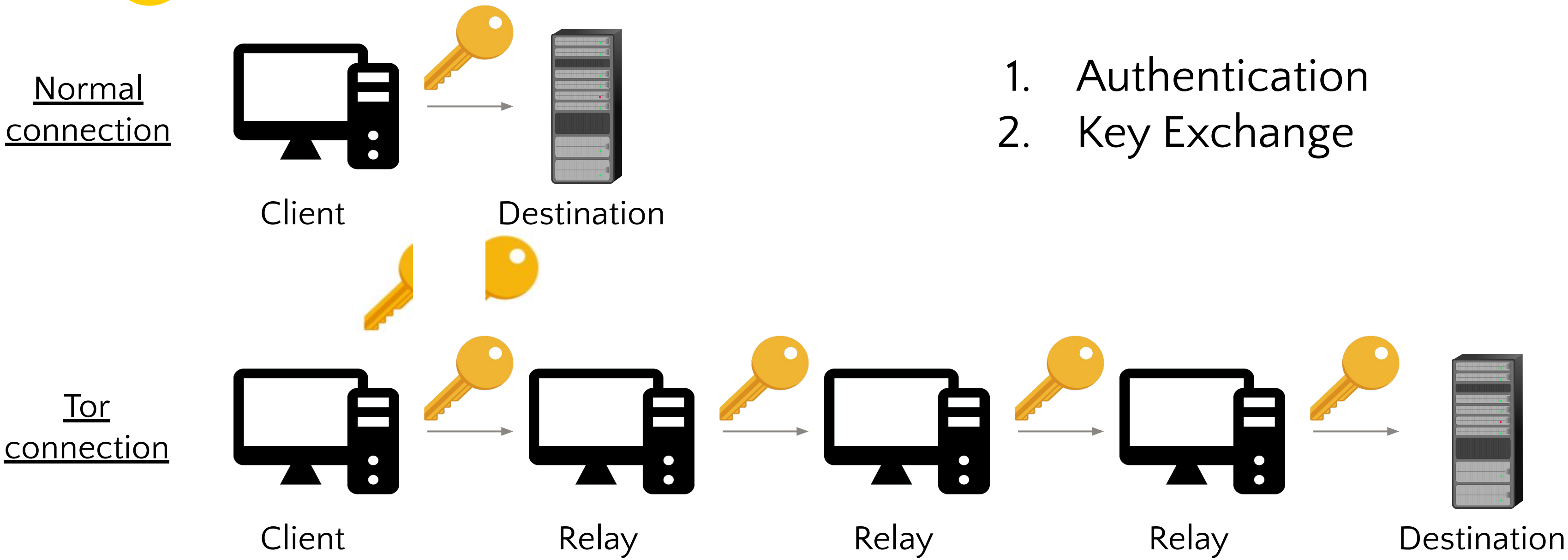
Destination

Why Handshake?



1. Authentication
2. Key Exchange

Why Handshake?



Normal connection

Client

Destination

Tor connection

Client

Relay

Relay

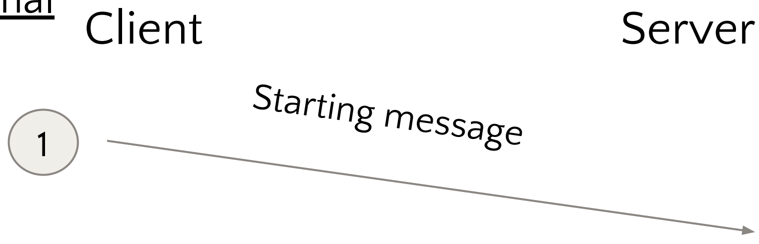
Relay

Destination

1. Authentication
2. Key Exchange

Handshakes

Normal



Client

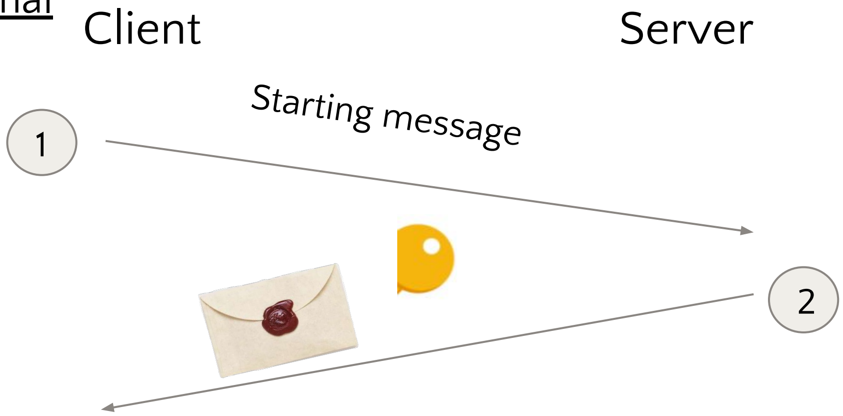
Server

1

Starting message

Handshakes

Normal



Client

Server

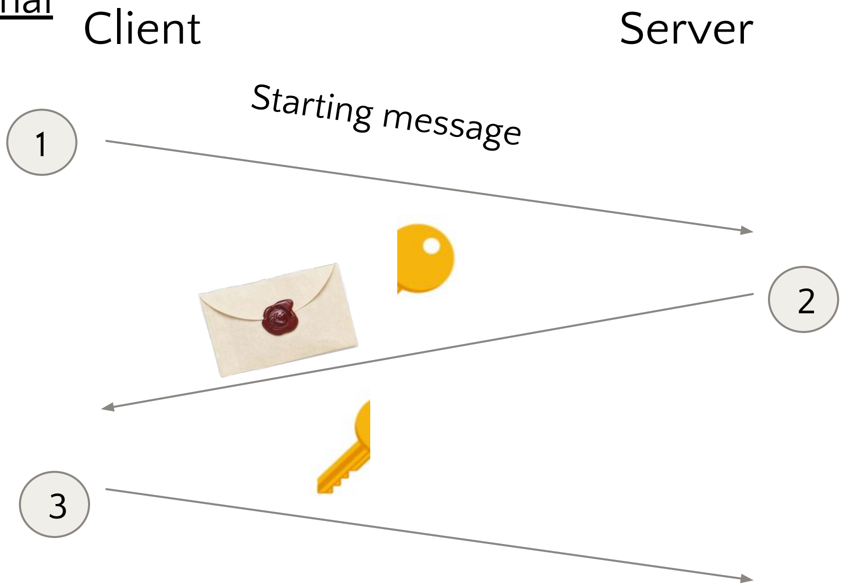
Starting message

1

2

Handshakes

Normal



Client

Server

Starting message

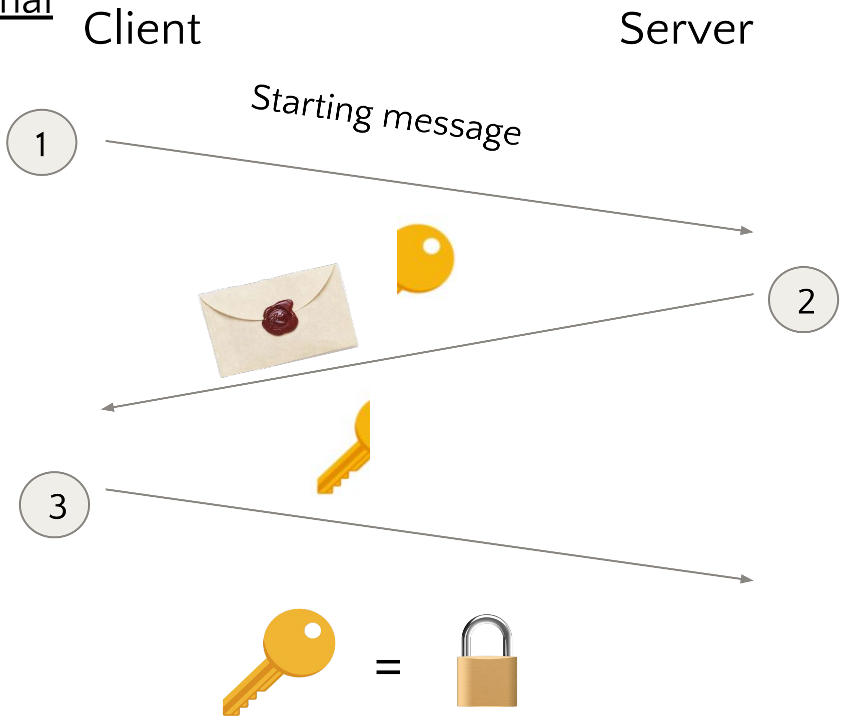
1

2

3

Handshakes

Normal



Client

Server

1

Starting message

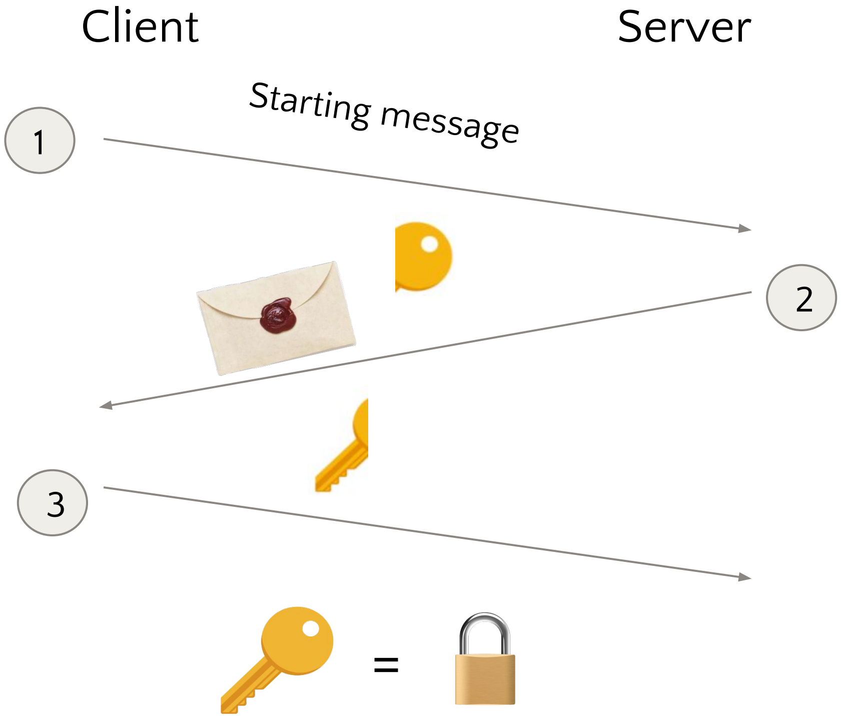
2

3

=

Handshakes

Tor



Client

Server

1

Starting message

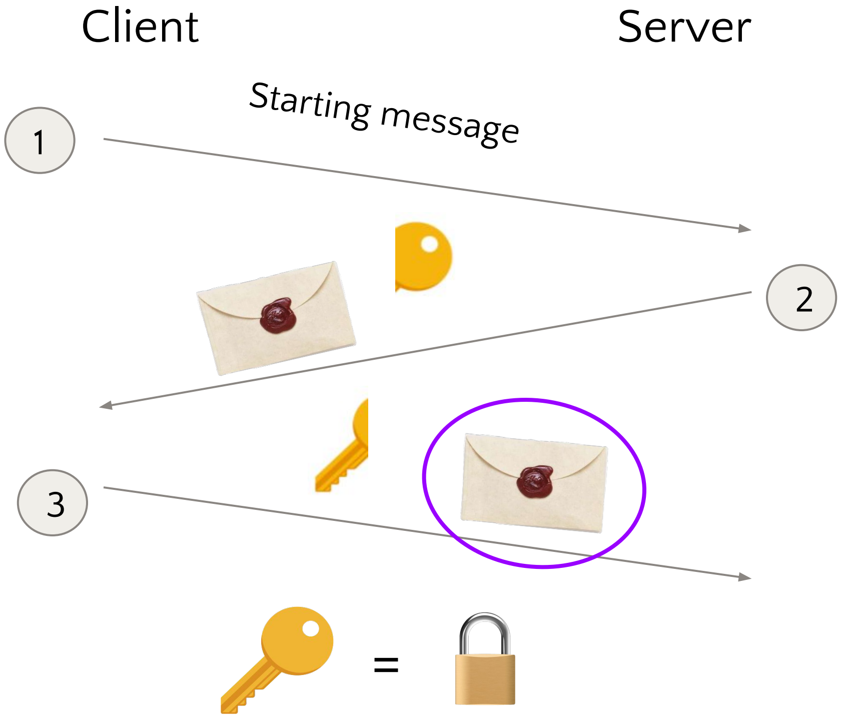
2

3

=

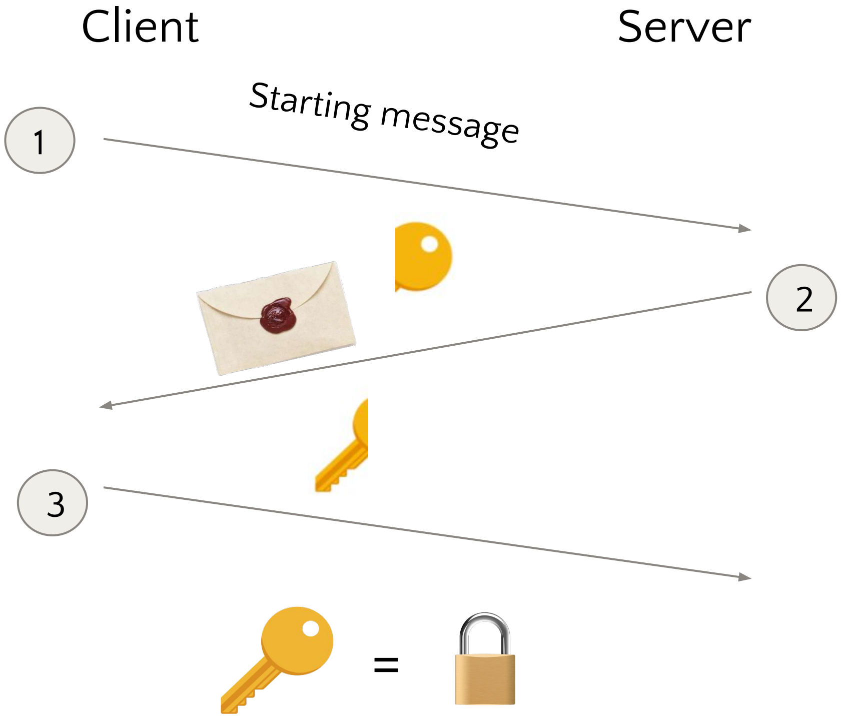
Handshakes

Tor



Handshakes

Tor



Client

Server

Starting message

1

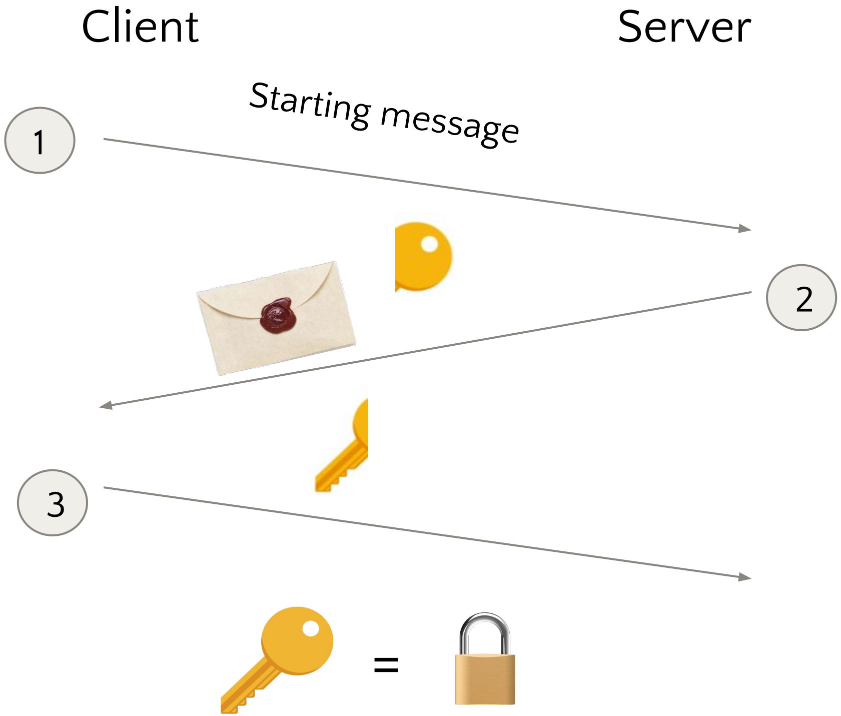
2

3

=

Handshakes

Tor



Client

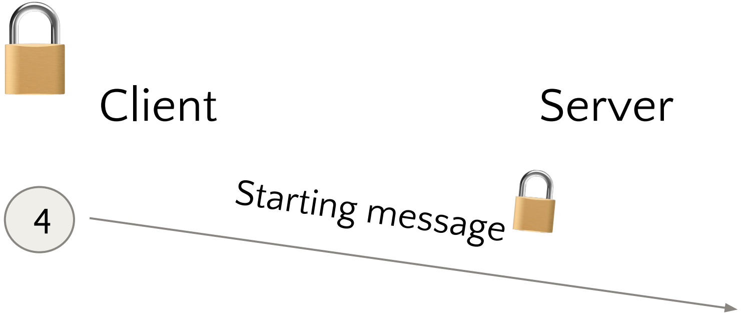
Server

1 Starting message

2

3

🔑 = 🔒



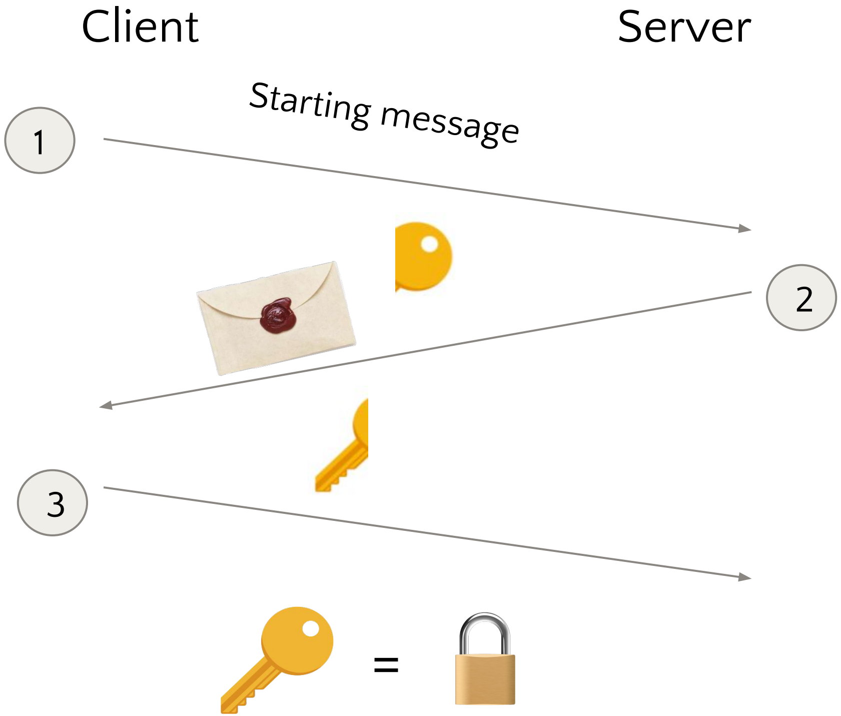
Client

Server

4 Starting message 🔒

Handshakes

Tor



Client

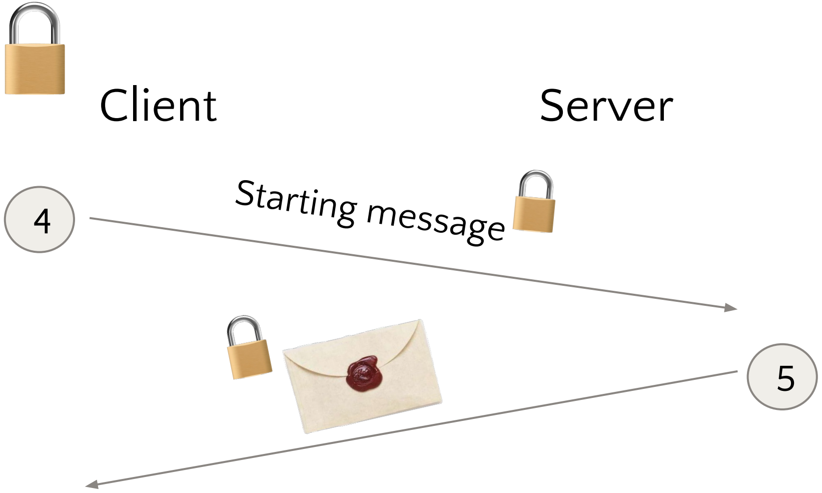
Server

1 Starting message

2

3

=



Client

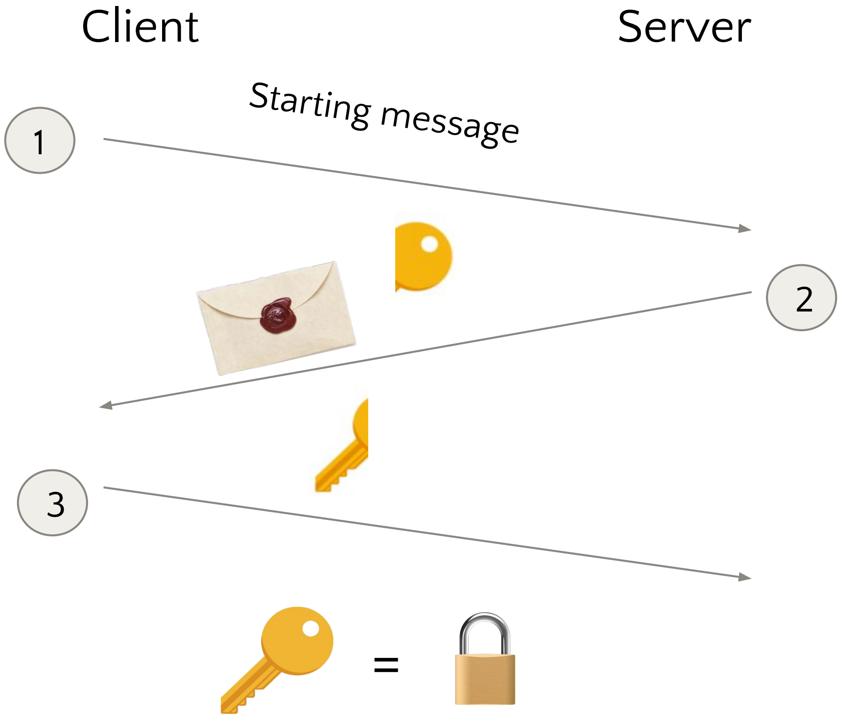
Server

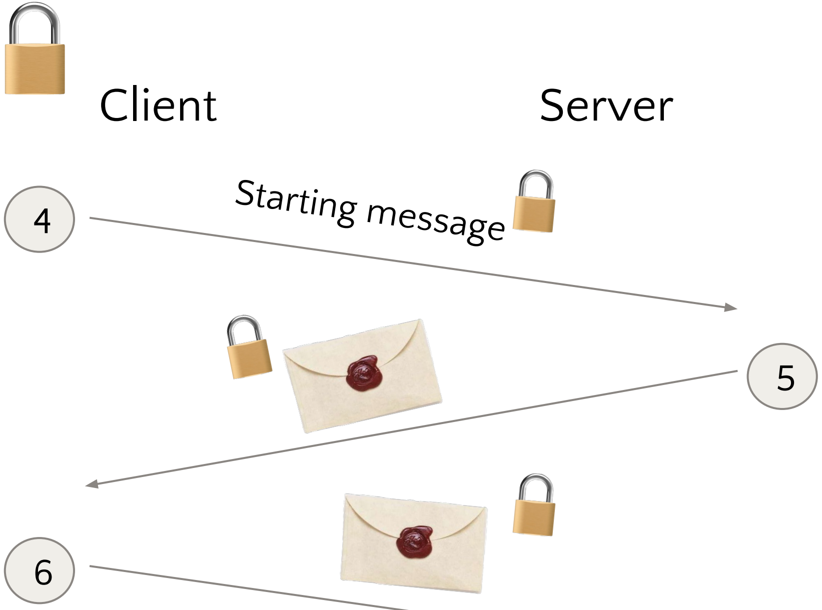
4 Starting message

5

Handshakes

Tor





3

Improvements

Improvements

Performance

Round trips

Bandwidth: Data being sent

Improvements

Performance

Round trips

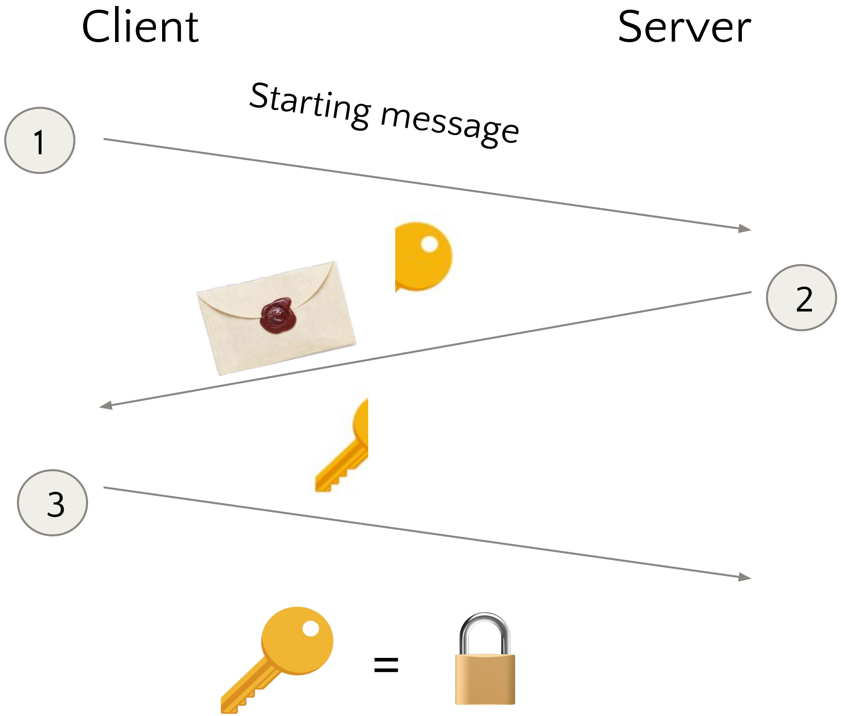
Bandwidth: Data being sent

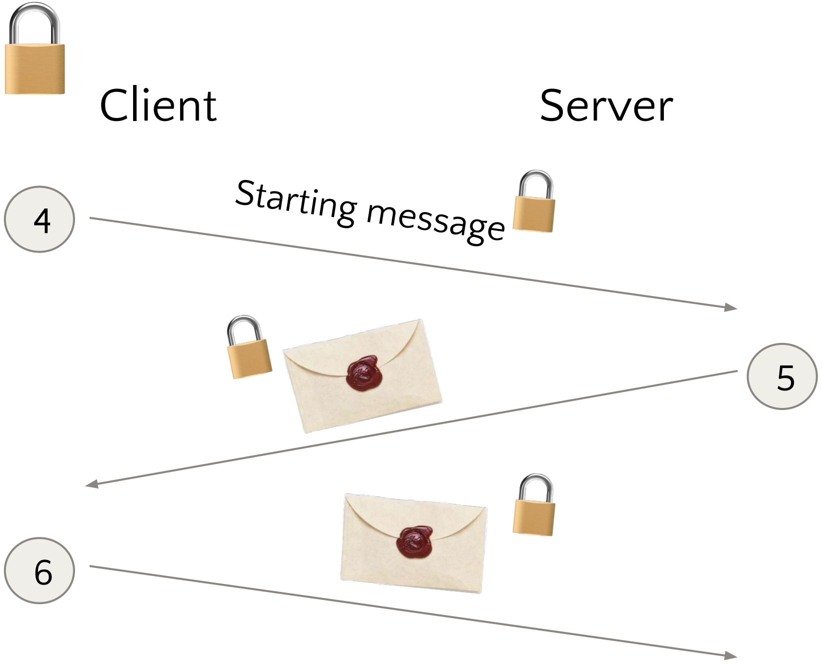
Security

Sensitive information being leaked

Removing Handshake Redundancy

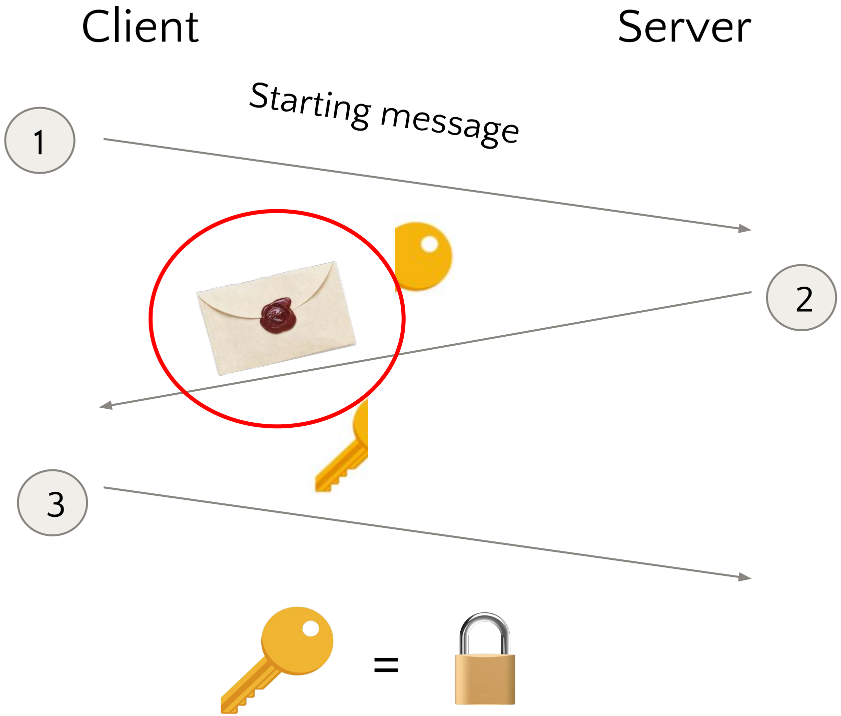
Tor





Removing Handshake Redundancy

Tor



Client

Server

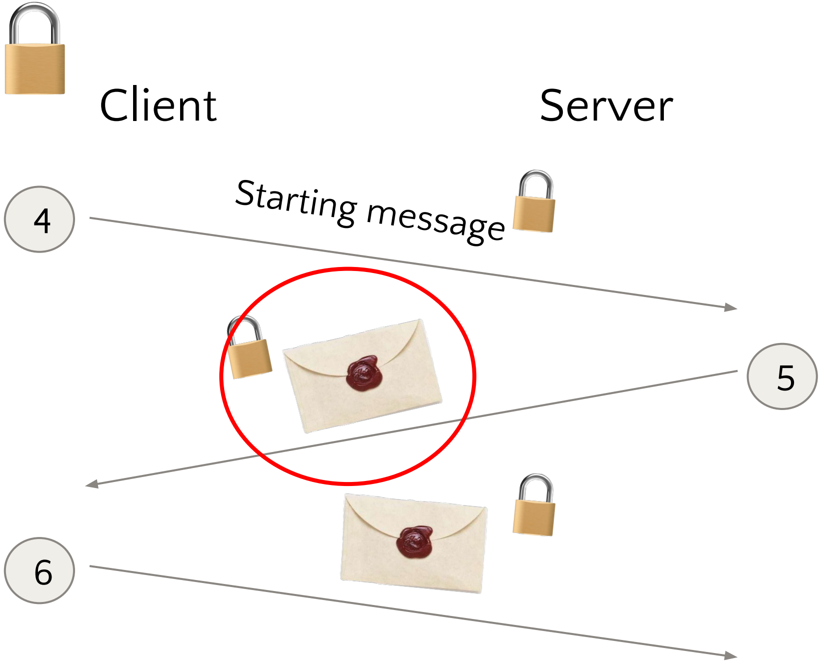
Starting message

1

2

3

=



Client

Server

Starting message

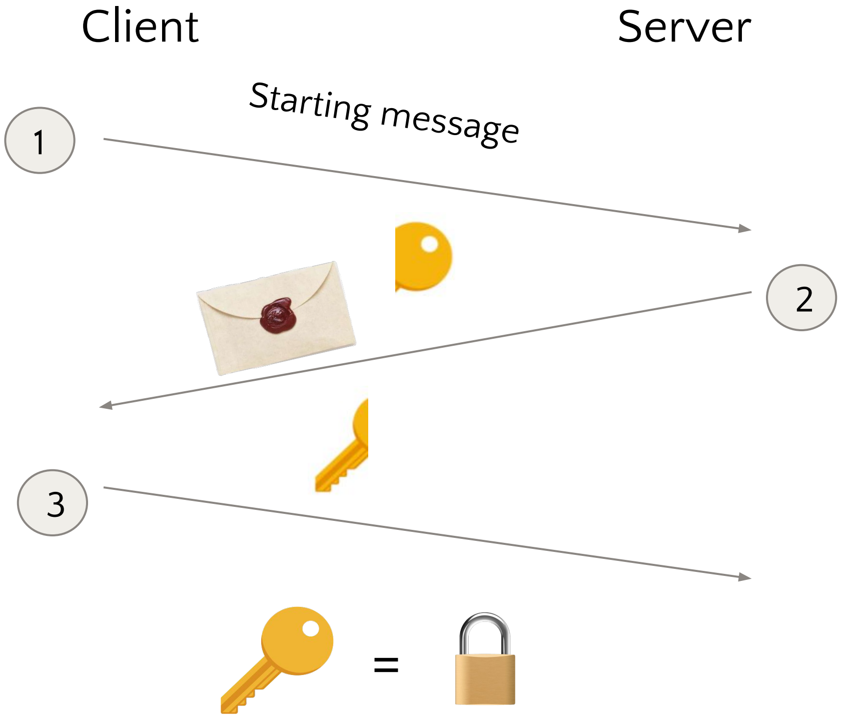
4

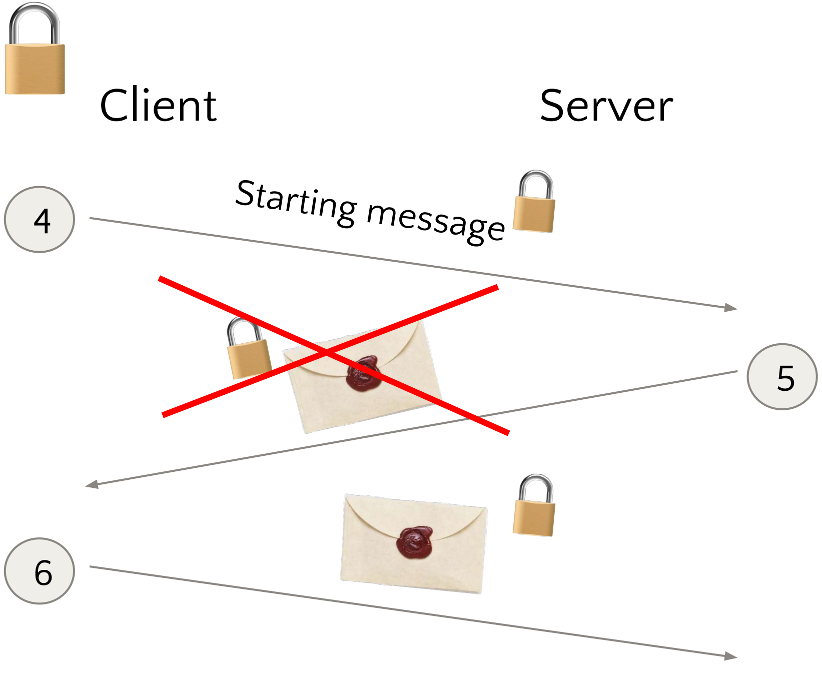
5

6

Removing Handshake Redundancy

Tor



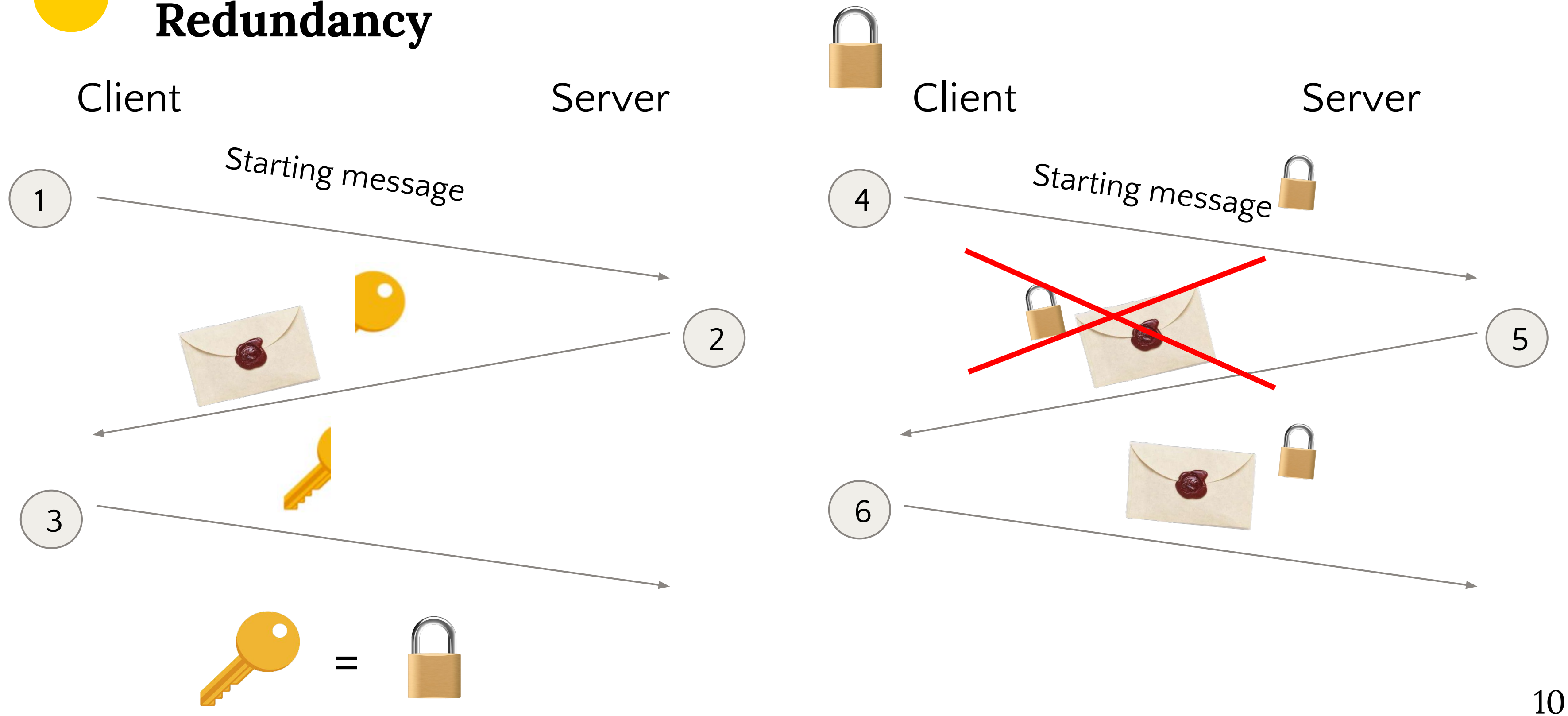


Performance

Bandwidth: Data being sent

Removing Handshake Redundancy

Tor



Client

Server

1 Starting message

2

3

=

Client

Server

4 Starting message

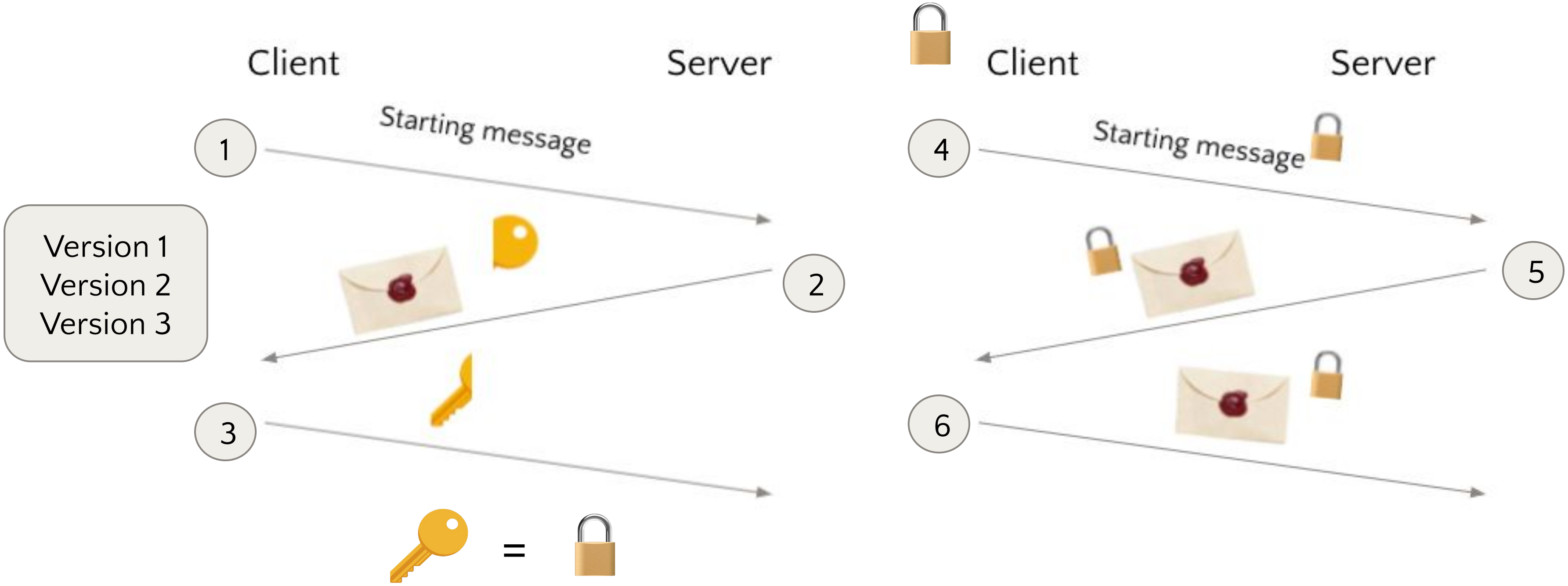
5

6

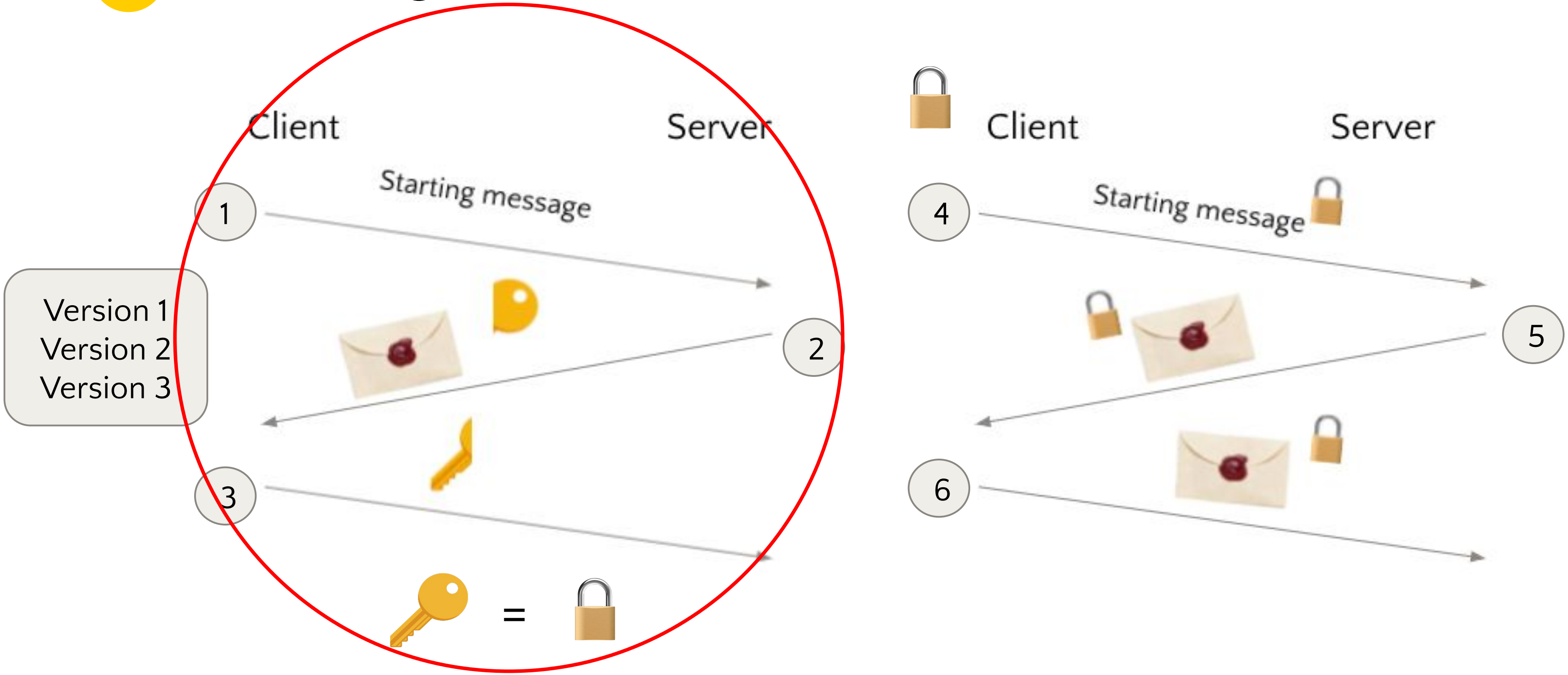
Removing Old Versions of Tor

Version 1
Version 2
Version 3

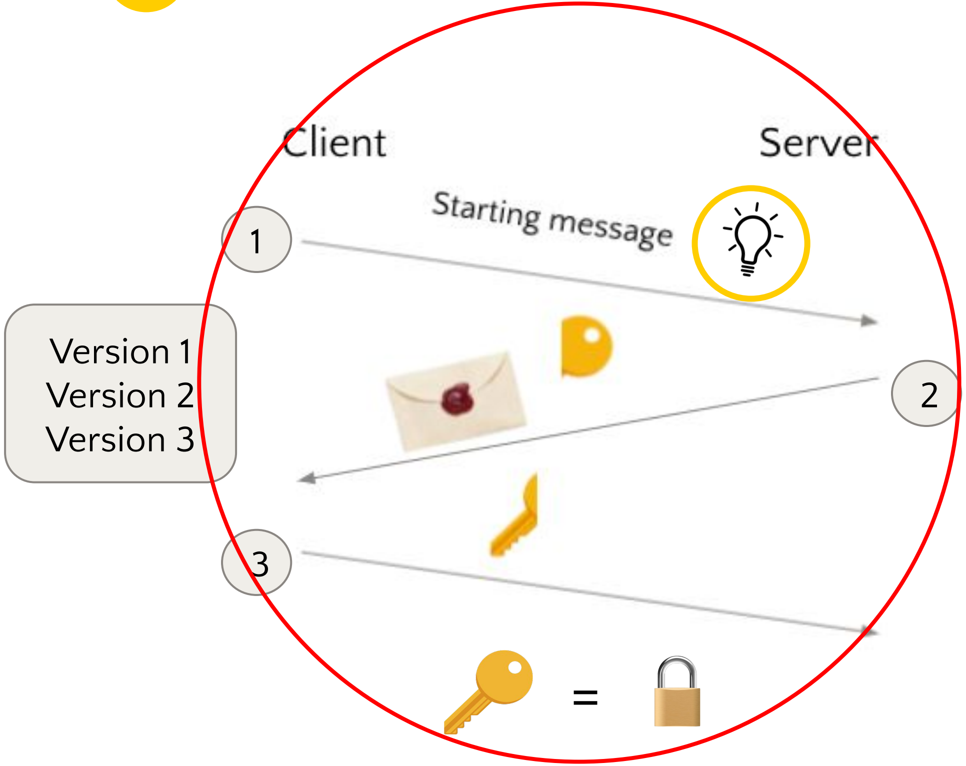
Removing Old Versions of Tor

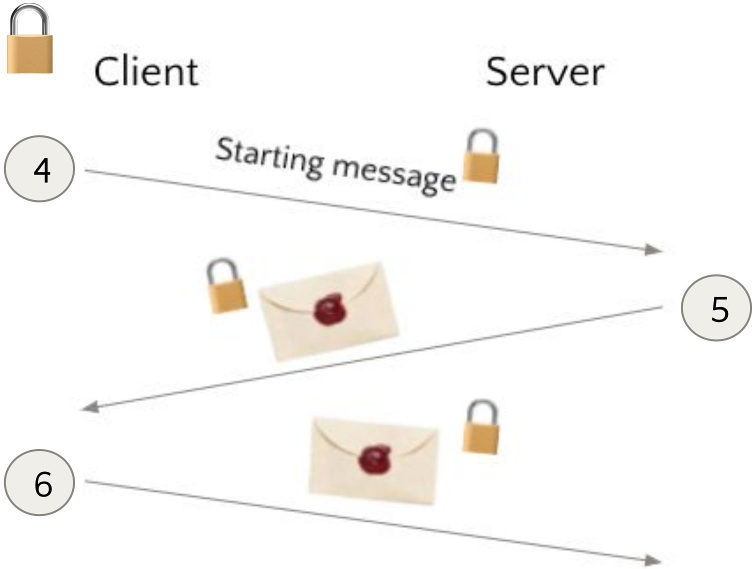


Removing Old Versions of Tor



Removing Old Versions of Tor

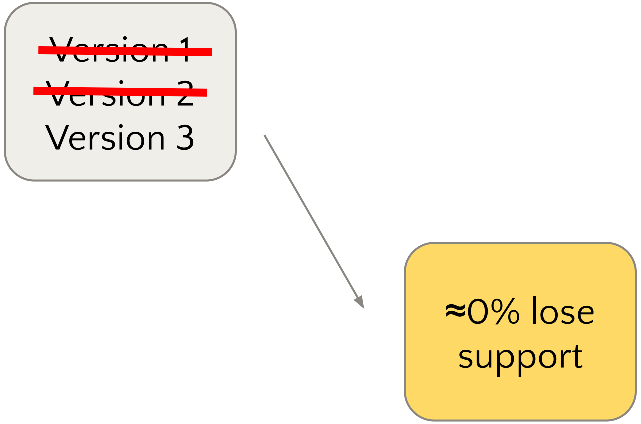




Removing Old Versions of Tor

Version 1
Version 2
Version 3

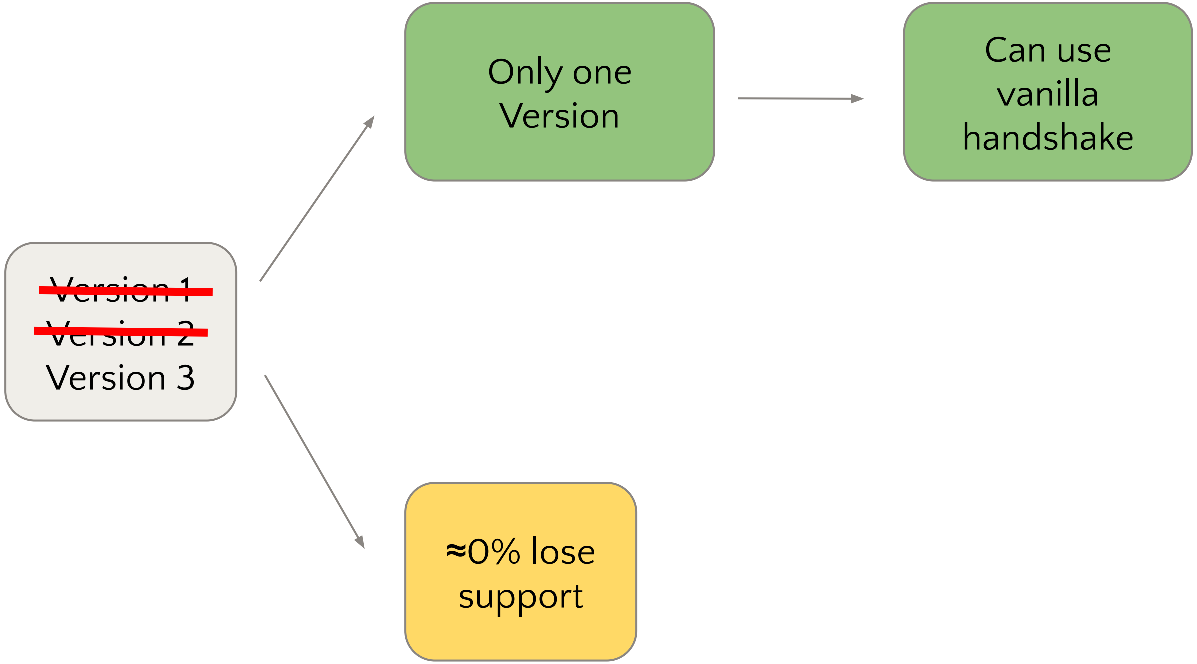
Removing Old Versions of Tor



~~Version 1~~
~~Version 2~~
Version 3

≈0% lose support

Removing Old Versions of Tor

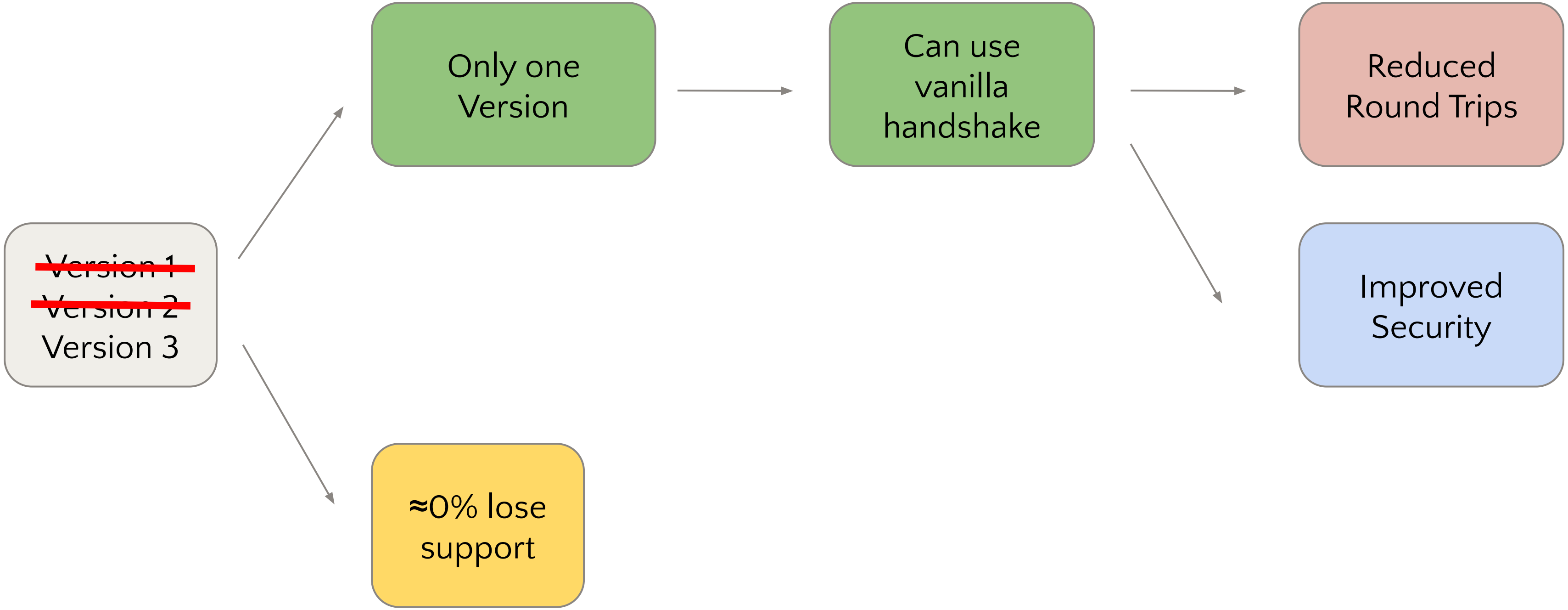

~~Version 1~~
~~Version 2~~
Version 3

Only one Version

Can use vanilla handshake

≈0% lose support

Removing Old Versions of Tor



~~Version 1~~
~~Version 2~~
Version 3

Only one Version

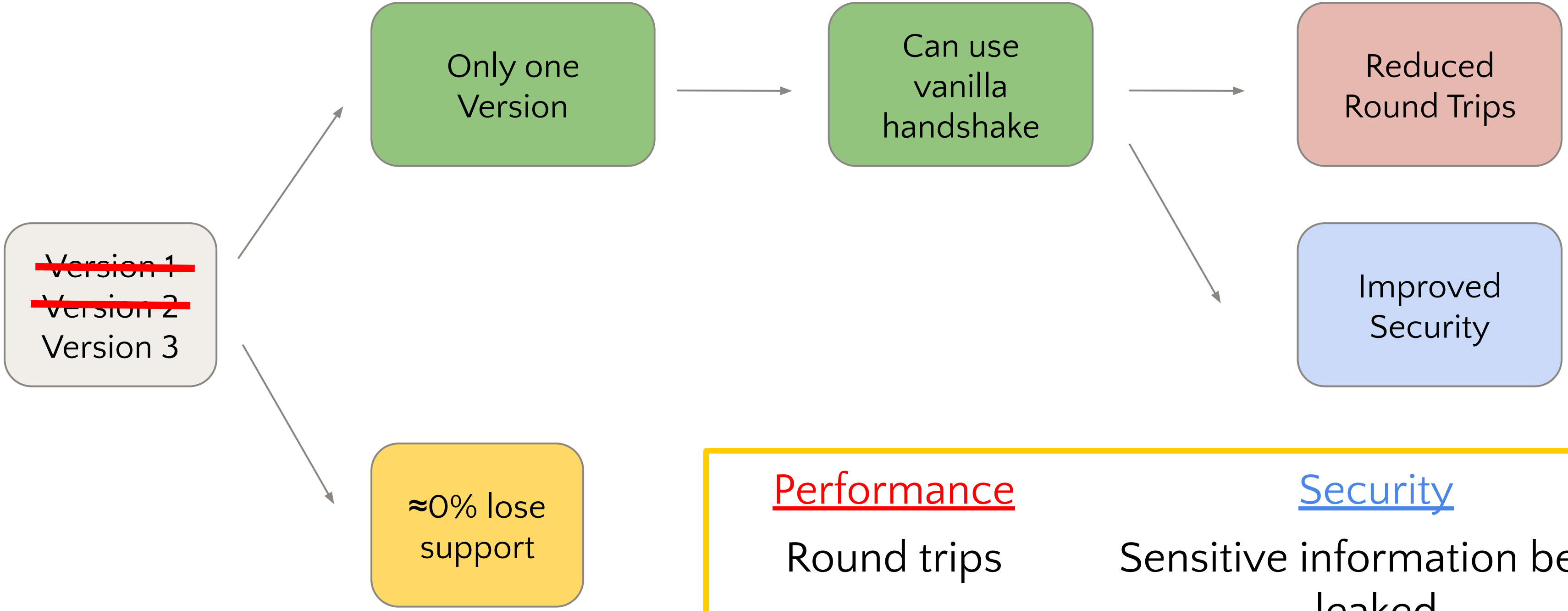
Can use vanilla handshake

Reduced Round Trips

Improved Security

≈0% lose support

Removing Old Versions of Tor



~~Version 1~~
~~Version 2~~
Version 3

Only one Version

Can use vanilla handshake

Reduced Round Trips

Improved Security

≈0% lose support

Performance

Round trips

Security

Sensitive information being leaked

Takeaways

Tor uses relays to achieve anonymity

Tor has a special handshake that hides two-way authentication

We propose 2 improvements to Tor’s handshake

- Removing extra certificate
- Removing old versions of Tor

Acknowledgements

Thank you to:

- My Mentor: Kyle Hogan
- Cristina Nita-Rotaru
- PRIMES
- My family