Passive and Active
Measurement Conference 2023

Measuring the Performance of iCloud Private Relay

Martino Trevisan, Idilio Drago,
Paul Schmitt, Francesco Bronzino

UNIVERSITÀ DEGLI STUDI DI TRIESTE

UNIVERSITY of HAWAI'I MĀNOA

UNIVERSITÀ DI TORINO

ENS DE LYON

Context

Context: a more private web

At the beginning of the Internet everything was **in clear**

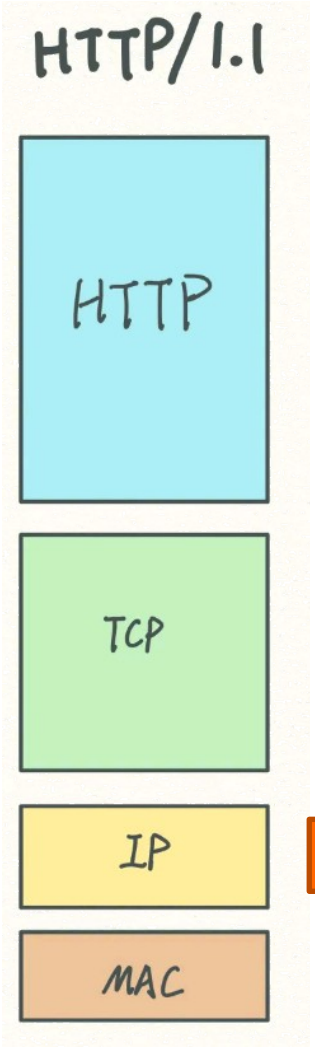
In clear traffic has **problems**

- For Security: Passwords, Credit Cards Numbers, etc.
- For Privacy: An Eavesdropper can observe your traffic, your websites, your interests

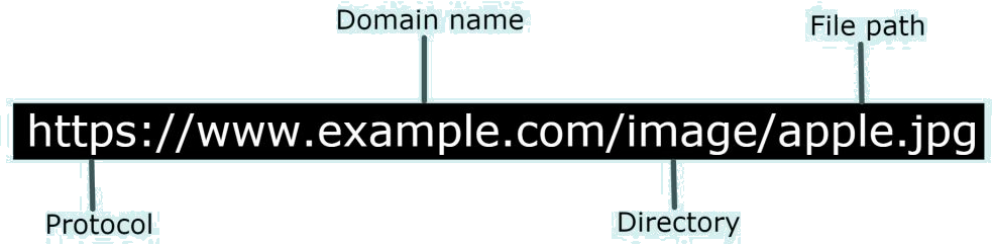
Since 2010, we observe a trend towards **encryption**

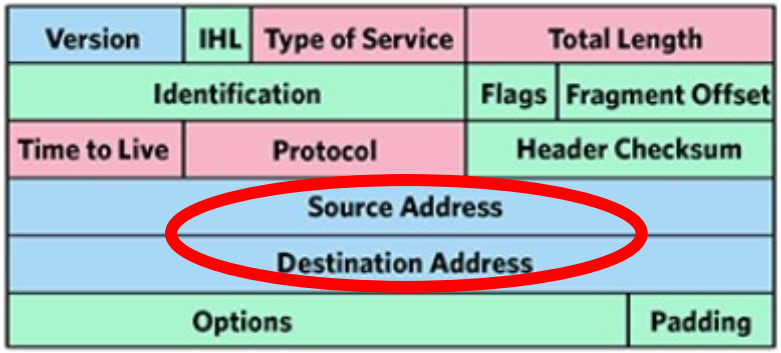
- More and more protocol fields get encrypted

Context: a more private web



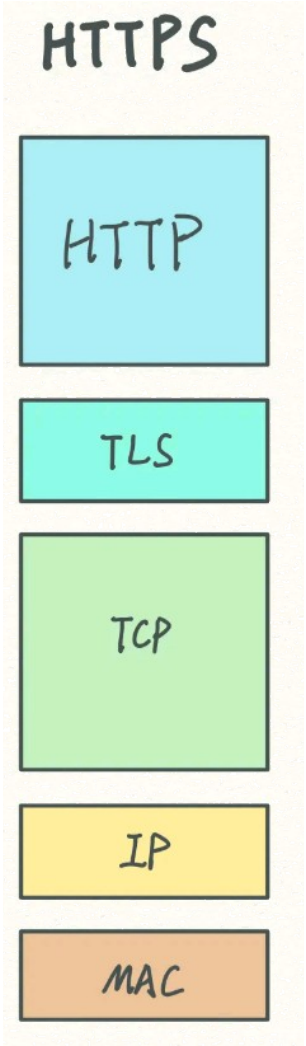
In clear URL





In clear Client and Server IP addresses

Context: a more private web



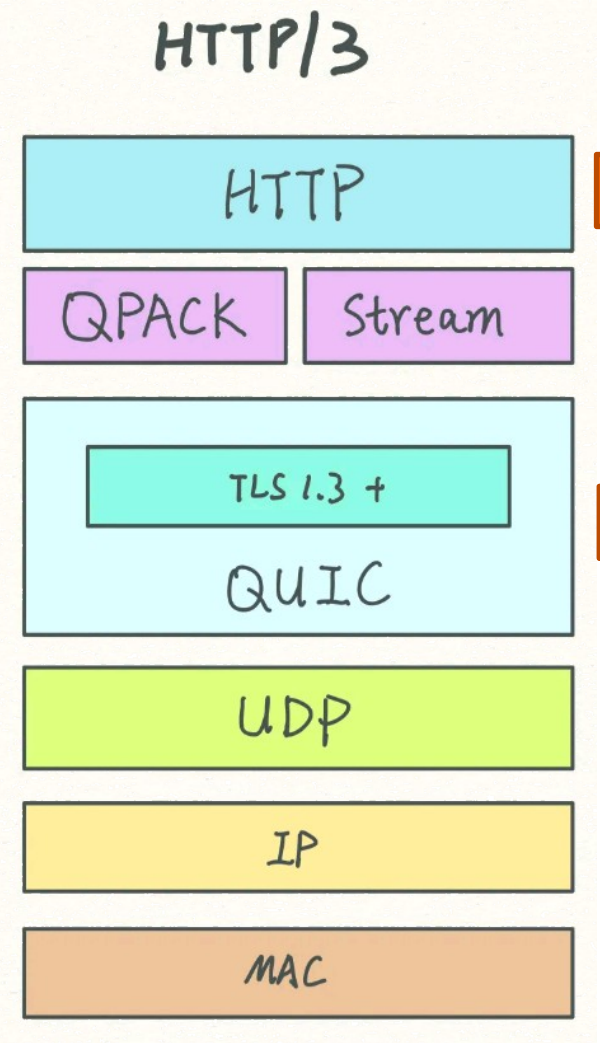
Encrypted

In clear Domain Name

```
Extension: server_name
    Type: server_name (0x0000)
    Length: 31
  Server Name Indication extension
      Server Name list length: 29
      Server Name Type: host_name (0)
      Server Name length: 26
      Server Name: tiles.services.mozilla.com
```

In clear Client and Server IP addresses

Context: a more private web



Encrypted

Encrypted Domain Name

`draft-ietf-tls-esni`

Workgroup: tls
Internet-Draft: draft-ietf-tls-esni-15
Published: 3 October 2022
Intended Status: Standards Track
Expires: 6 April 2023

E. Rescorla
RTFM, Inc.
K. Oku
Fastly
N. Sullivan
Cloudflare
C. A. Wood
Cloudflare

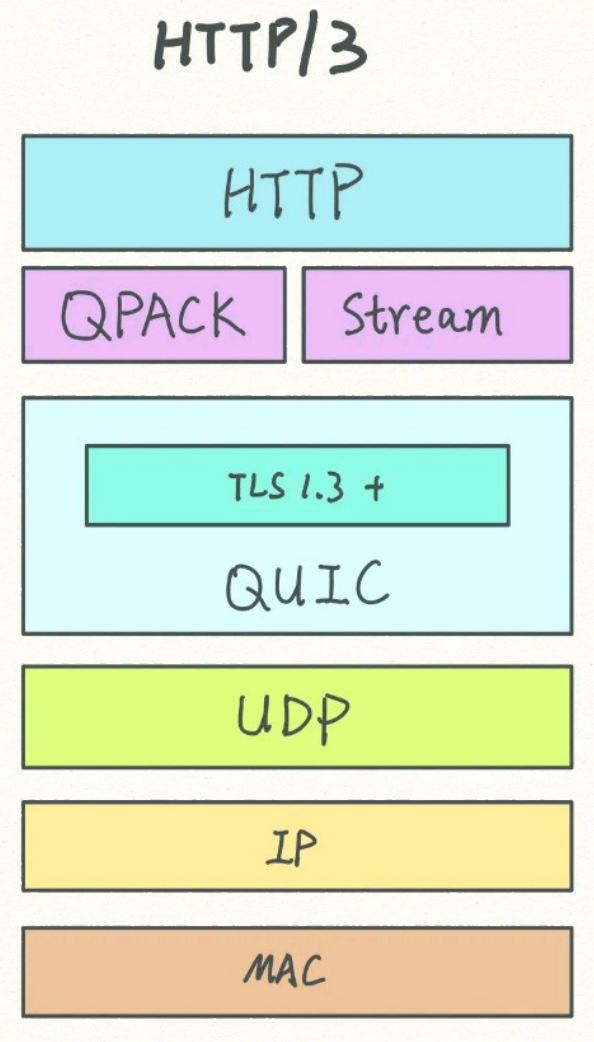
TLS Encrypted Client Hello

Abstract

This document describes a mechanism in Transport Layer Security (TLS) for encrypting a ClientHello message under a server public key.

In clear Client and Server IP addresses

Context: a more private web



The ISP knows visited servers

- And possibly the website

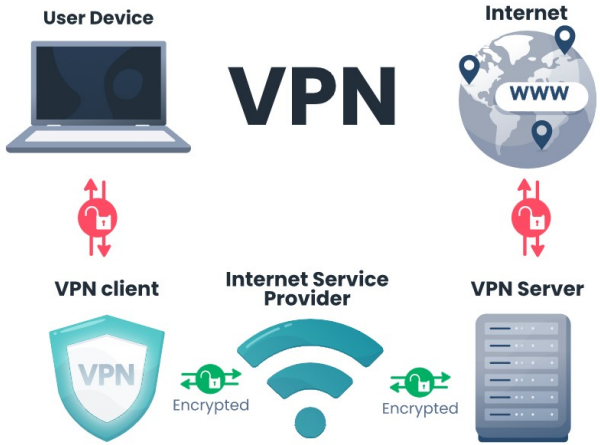
The website knows audience's IP

- Can track them

In clear Client and Server IP addresses

Solution: anonymity services!

- **Virtual Private Networks**



Network Working Group
Request for Comments: 1825
Category: Standards Track

R. Atkinson
Naval Research Laboratory
August 1995

Security Architecture for the Internet Protocol

- **Developed in the mid-1990s by United States Naval Research Laboratory**

IP addresses are encrypted!

iCloud Private Relay

Solution: The Apple Way

iCloud Private Relay

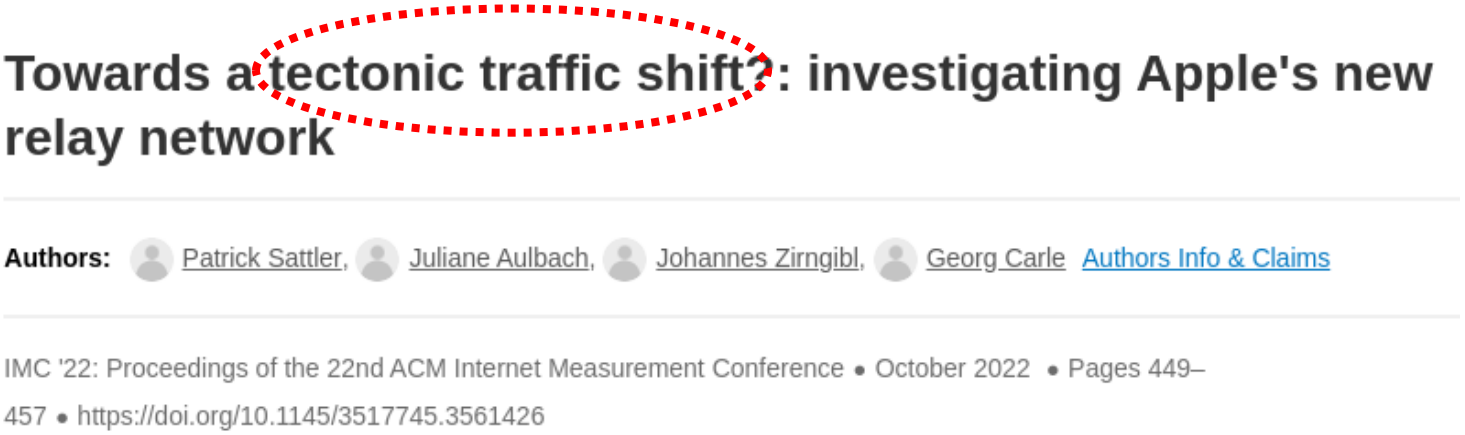
- Launched in 2021
- Included in iCloud+ plan
- VPN-like service
- Integrated in MacOS and iOS
- Easy to use

iCloud

Private Relay: Interesting to study

Can become widely deployed!

- Low entry barriers
- E.g., 25% of smartphones are iPhone!
- ➢ **Implications on the global traffic mixture!**



Towards a tectonic traffic shift?: investigating Apple's new relay network

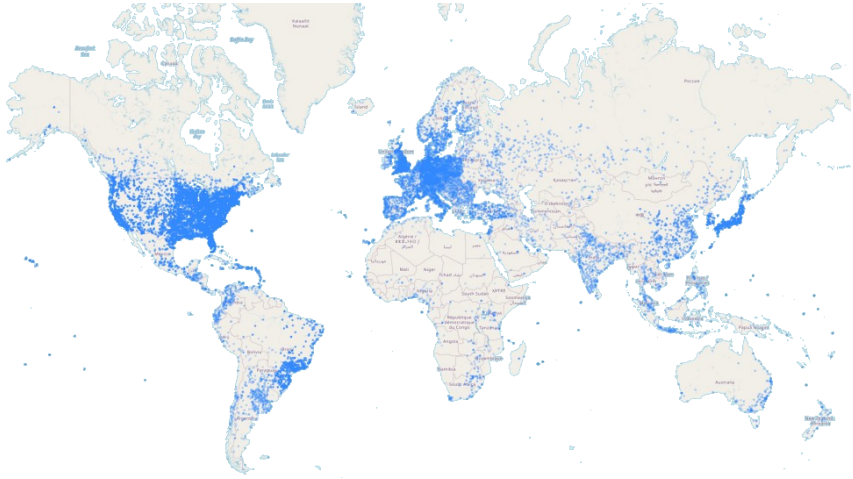
Authors: Patrick Sattler, Juliane Aulbach, Johannes Zirngibl, Georg Carle Authors Info & Claims

IMC '22: Proceedings of the 22nd ACM Internet Measurement Conference • October 2022 • Pages 449–457 • https://doi.org/10.1145/3517745.3561426

Private Relay: Interesting to study

Large infrastructure already deployed

- Based on Akamai, Cloudflare and Fastly
- Apple declares 238 k subnets
- ➢ Complications for **GeoBlocking** services



Towards a tectonic traffic shift?: investigating Apple's new relay network

Authors: Patrick Sattler, Juliane Aulbach, Johannes Zirngibl, Georg Carle Authors Info & Claims

IMC '22: Proceedings of the 22nd ACM Internet Measurement Conference • October 2022 • Pages 449–457 • https://doi.org/10.1145/3517745.3561426

Private Relay: Interesting to study

Novel Technical Operation

Two-Hop architecture

- Traffic passes through **two proxies** before reaching the server

Based on QUIC

- Implementes novel features of **QUIC**

Private Relay: Two-Hop Architecture

Multi-Party Relay architecture

Decouples:

- Users' network identity: Client IP
- Internet usage: Server IP

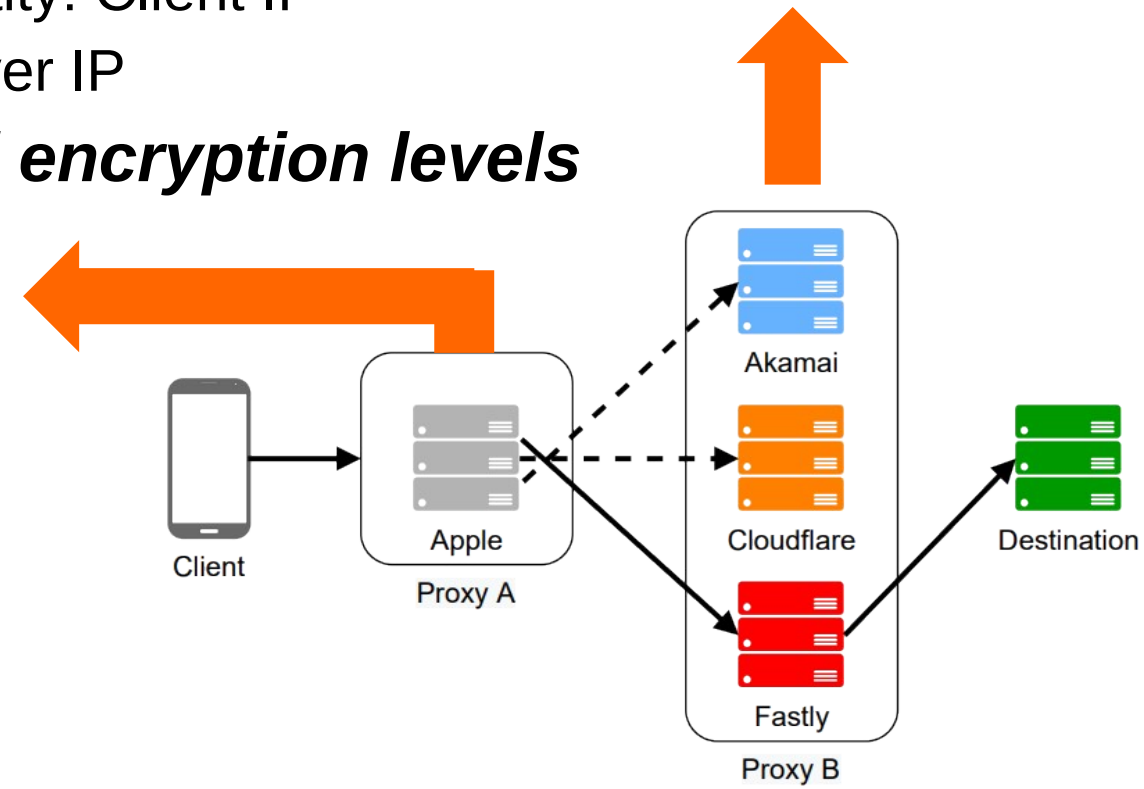
Based on ***2 nested encryption levels***

Does not know *Client* IP

Knows *Server* IP

Knows *Client* IP

Does not know *Server* IP



Private Relay: Based on QUIC

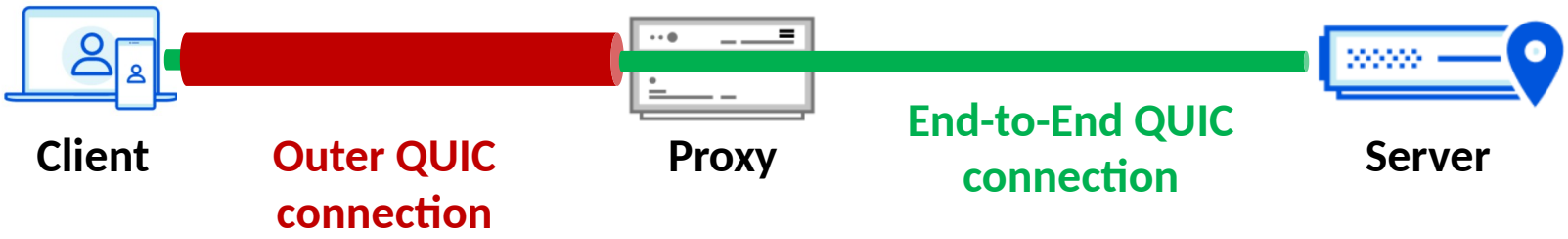
The two nested encryption levels are **QUIC** connections

- With **modifications** to avoid **pitfalls**
  - First commercial use of **two recent RFCs**

- **Issue 1:** two nested instances of **reliable** protocols
- **Issue 2:** must create a **CONNECT** equivalent for QUIC
  - Solution: **RFC9220**: Extended Connect for QUIC

Private Relay: Based on QUIC

- **Issue 1:** two nested instances of reliable protocols:
  - Known to be a bad idea: Long delays and frequent connection aborts are to be expected
  - **Outer QUIC connection**: Client <-> Proxy
  - **End-to-End QUIC connection**: Client <-> Server
- **Solution**: use QUIC's unreliable datagram extension (RFC9221) also called **MASQUE**
  - Disable retransmissions **in Outer QUIC connection** : Client <-> Proxy
    - Useless as provided in **End-to-End QUIC connection**



Goal and Methods

Goal of the paper: Performance

Research Question: is there a performance penalty when using iCloud Private Relay?

- Slower Throughput?
- Downloading files takes more time?
- Web pages load more slowly?

Experimental Setup

Three MacOS PCs

Trieste (IT)

Lyon (FR)

Honolulu (US)

- Connected via **Ethernet** to the Internet
- Payed **Subscription** to iCloud Private Relay

Experimental Setup

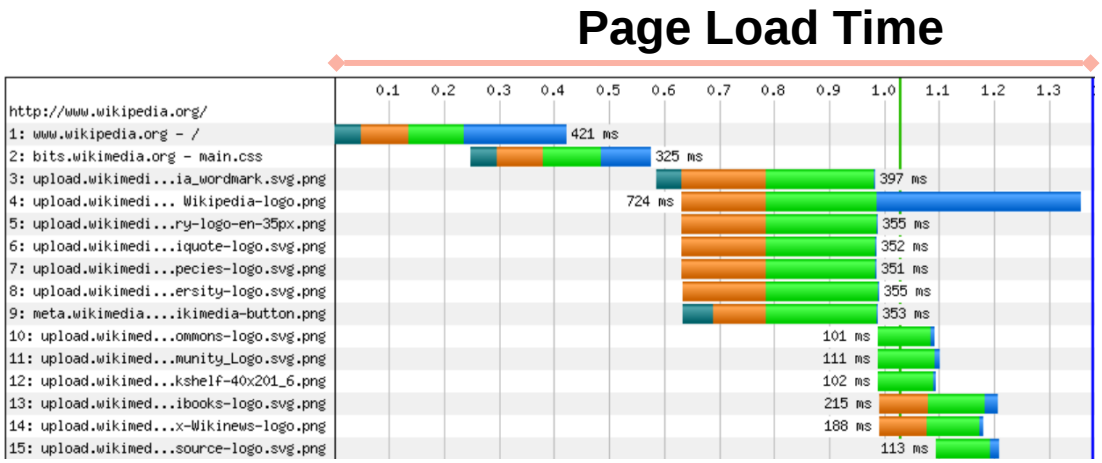
Three set of experiments

1. **Throughput Measurements**: via Ookla Speed Test
   - **KPI**: Download/Upload Throughput

2. **Bulk Download**: of a 1 GB test file on Hetzner CDN
   - **KPI**: Download Speed

Experimental Setup

3. **Web Browsing**: visit top-100 websites per country
   - Using **Safari**
   - **Automated** with BrowserTime testing tools
   - **KPI**: Page Load Time:
     - Time between first and last HTTP request



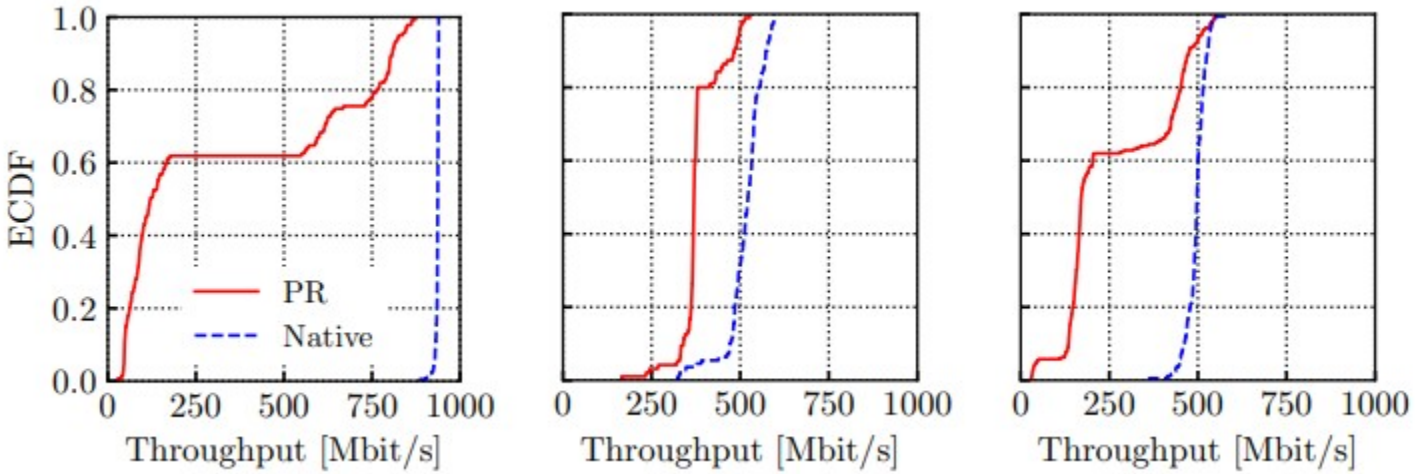
   - Correlated with Users's Quality of Experience

Experimental Results

Results: Throughput

Download:

- PR is not as fast as native network!

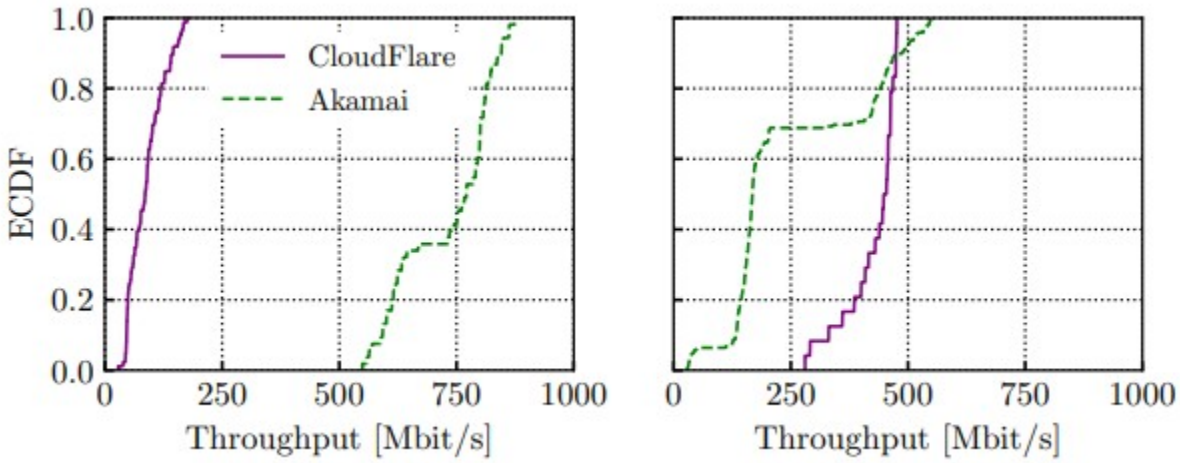


France **Italy** **US**

Results: Throughput

Download:

- Performance varies depending on the Proxy owner!

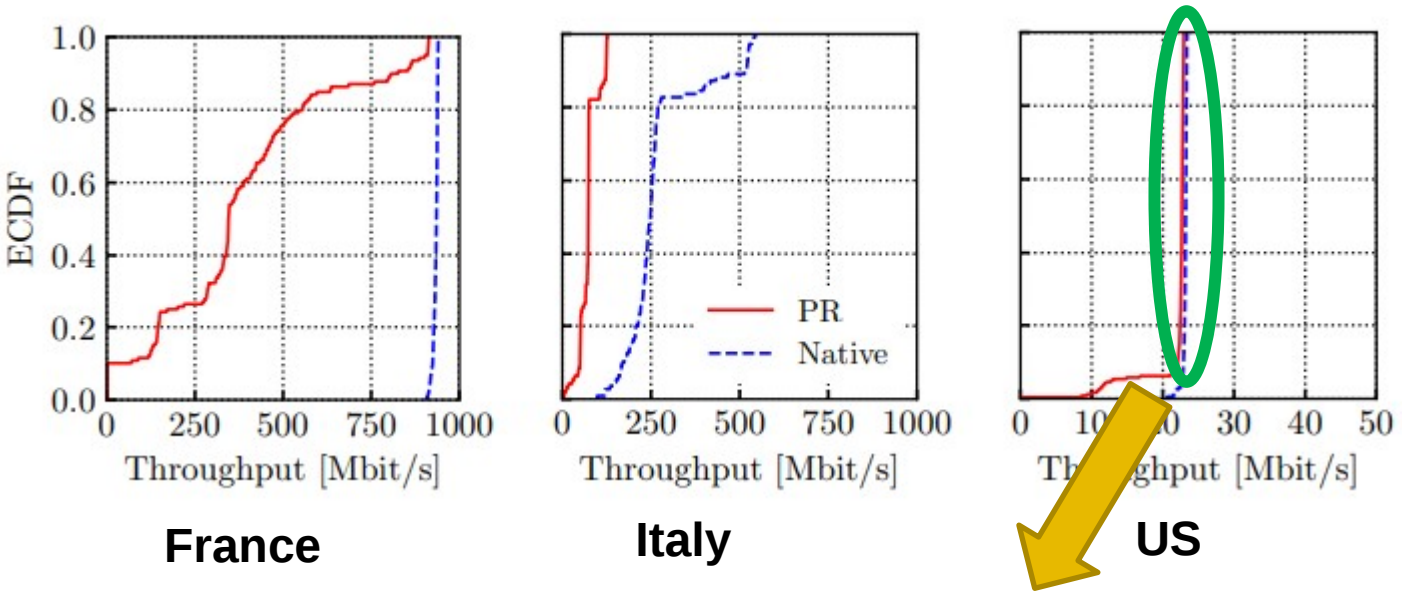


France **US**

Results: Throughput

Upload:

- Again PR is not as fast as native network!

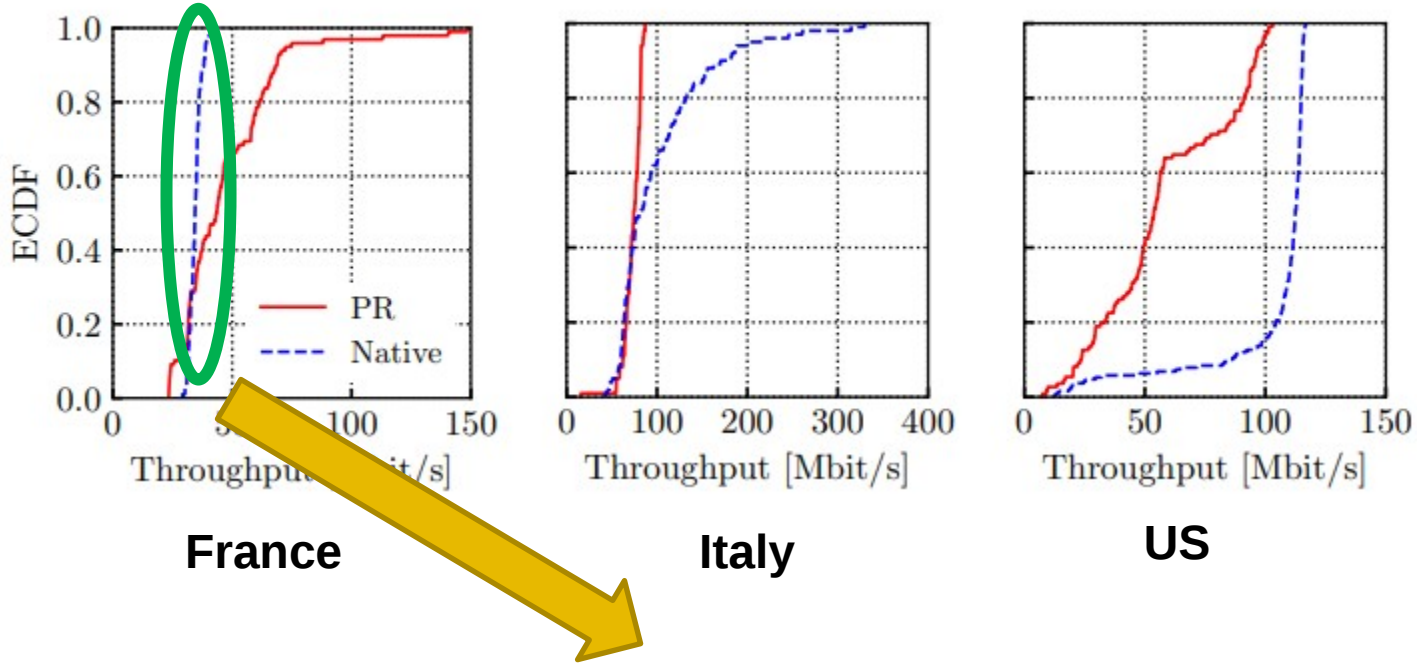


France **Italy** **US**

Slow Uplink is the bottleneck!

Results: Bulk Download

No clear winner

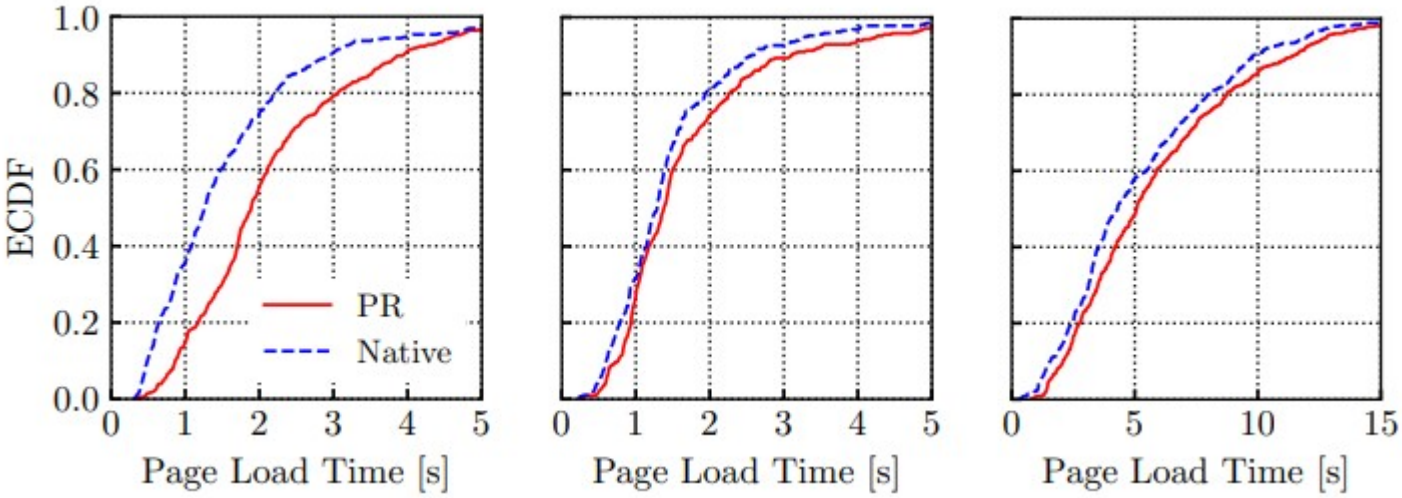


France **Italy** **US**

Cannot find root cause!

Results: Web Browsing

Page Load Time **larger** by 7-60%



France **Italy** **US**

Final Remarks

iCloud Private Relay moderately impairs performance

- First commercial use of new features
  - QUIC Datagrams / MASQUE

Other aspects left to study

- Implications on Localizations / Geo Blocking
- Cost
  - In terms of computing resources
  - Energy (for additional encryption)

Thank you for your attention