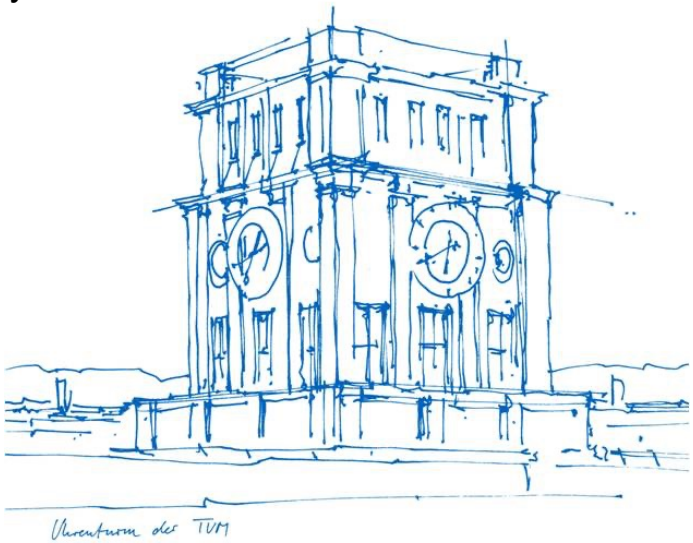
DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance

Mike Kosek, Luca Schumann, Trinh Viet Doan | Technical University of Munich

Robin Marx | KU Leuven

Vaibhav Bajpai | CISPA Helmholtz Center for Information Security

IMC 2022



See also previous paper

- “One to Rule them All? A First Look at DNS over QUIC” @ PAM 2022
- Presented at MAPRG @ IETF 113

- **Main differences** with today:
  - Updated DNS over QUIC implementation
    - Session resumption, 0-RTT, address validation/amplification prevention
  - Multiple vantage points
  - Added **Web Performance measurements**

Motivation

- Web traffic shifted to HTTPS
- Privacy leaks through unencrypted DNS over UDP (DoUDP) queries

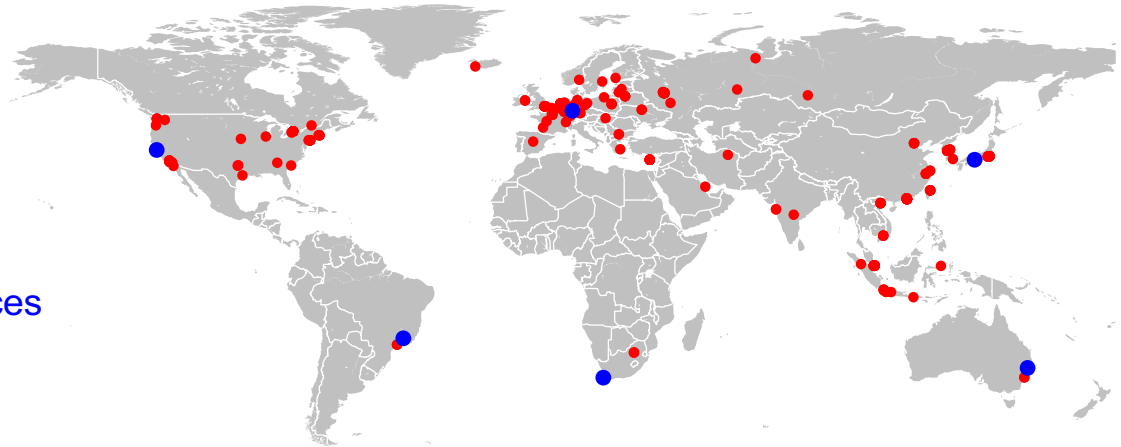
- Addressed by DNS over TLS (DoT) and DNS over HTTP/2 (DoH)
- Suboptimal performance due to **TCP+TLS handshake (2-RTT+)**

- QUIC combines connection and encryption into 0/1-RTT handshake
- DNS over QUIC (DoQ) aims to combine **DNS privacy with minimal latency**

Impact of DoQ on Web performance?

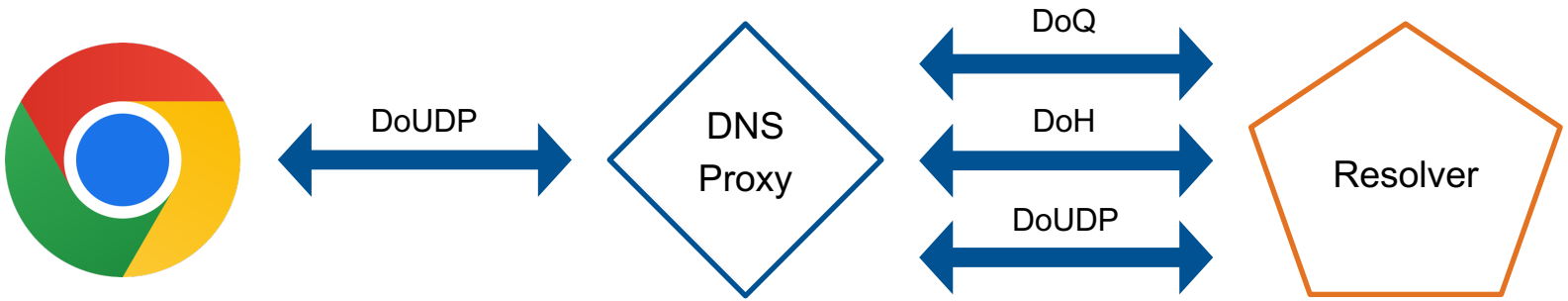
Target Resolvers and Vantage Points

- Target Resolvers
  - *ZMap* Scan of the IPv4 address space from a single VP in EU in April 2022
  - 1,216 DoQ resolvers, of which **313** support DoH and DoUDP
  - Geographical Distribution
    - EU: 130
    - AS: 128
    - NA: 49
    - AF/OC/SA: 2 each
- Vantage Points
  - 6 distributed Amazon EC2 instances



Methodology

- Tooling
  - *Selenium* with *Chromium:* **Top 10** most popular webpages (*Tranco April 12th 2022*)
  - *DNS Proxy:* DNS over QUIC / HTTPS / UDP *(and DoTCP, DoT)**



* https://github.com/justus237/dnsproxy

Methodology

- Tooling
  - *Selenium* with *Chromium:* **Top 10** most popular webpages (*Tranco April 12th 2022*)
  - *DNS Proxy:* DNS over QUIC / HTTPS / UDP *(and DoTCP, DoT)**
- Measurements
  - Every webpage (10) using each DNS protocol (3) via every resolver (313) from all vantage points (6)
  - Repeated every 48 hours over the course of one week in April 2022
  - **2 back-to-back navigations**: (a) cache warming, and (b) actual Web performance measurement
    - Populate DNS Cache of the resolver *(NOT the browser cache!)*
    - QUIC Version negotiation and Address Validation *(These DoQ servers always use RETRY ☹)*
    - TLS 1.3 Session Ticket

Evaluation – Measurement Overview

- Samples: DoQ: 57,393 / DoH: 56,840 / DoUDP: 57,032

- DNS over QUIC
  - TLS 1.3 Session Resumption 100%
  - 0-RTT 0%
  - QUIC Version *1* *89%* *(draft-34, -32, and -29)*
  - DoQ Draft Version *02* *87%.* *(doq-i03, doq-i00)*

Evaluation – Measurement Overview

- Samples: DoQ: 57,393 / DoH: 56,840 / DoUDP: 57,032

- DNS over QUIC
  - TLS 1.3 Session Resumption 100%
  - 0-RTT 0%
  - QUIC Version *1* *89%* *(draft-34, -32, and -29)*
  - DoQ Draft Version *02* *87%.* *(doq-i03, doq-i00)*

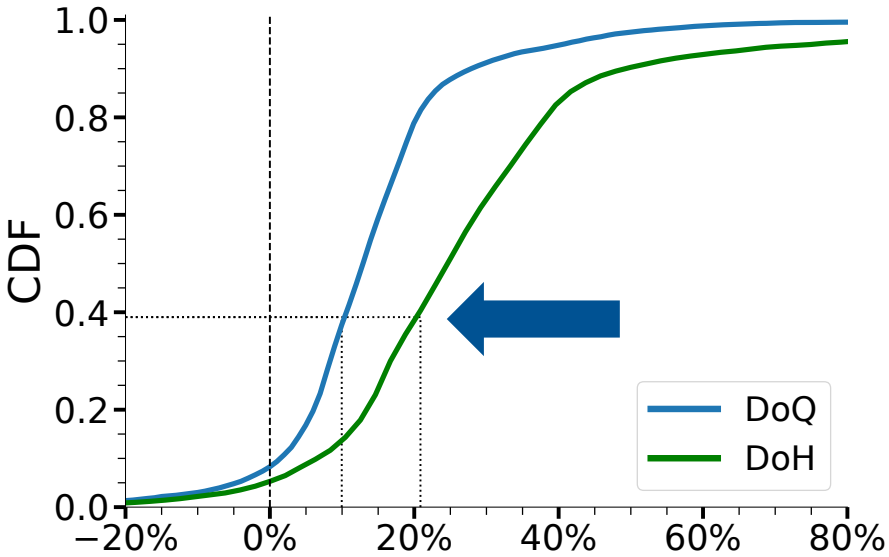
- DNS over HTTP/2
  - TLS 1.3 Session Resumption 99%
  - 0-RTT 0%
  - TCP Fast Open 0%
  - HTTP/2 100%

Evaluation – Metrics

- **First Contentful Paint**: time until the first visible image or text is shown on the screen
  - Early in the page load
  - Should correlate well with DNS perf

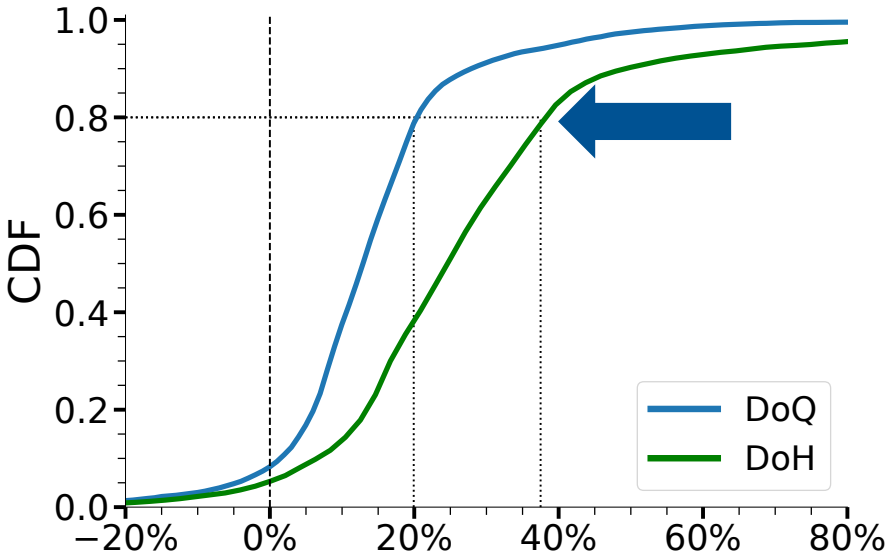
- **Page Load Time**: time until the start of the onLoad event
  - End of the page load
  - Might have worse correlation

Evaluation – First Contentful Paint over all webpages



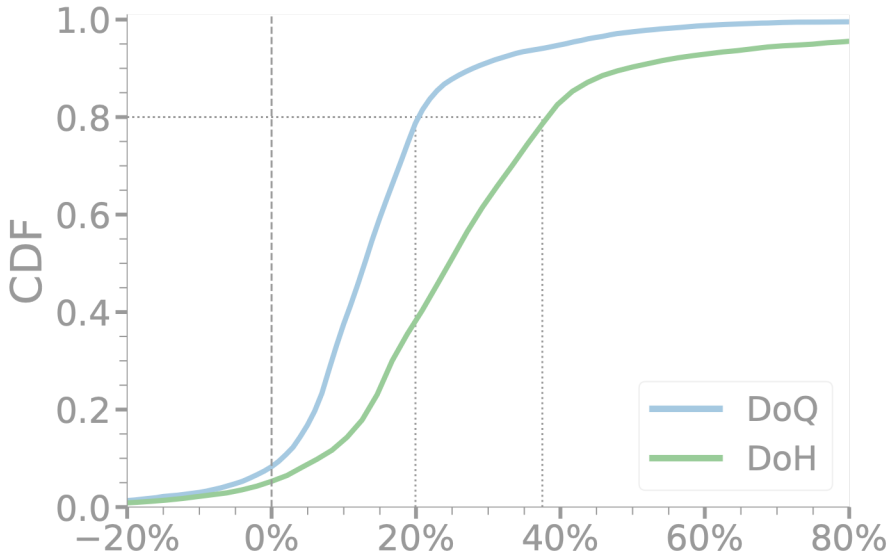
- Relative FCP differences between
  - DoUDP (baseline)
  - DoQ
  - DoH
- At **p40**, FCP increased by <= 10% for DoQ, 20% for DoH

Evaluation – First Contentful Paint over all webpages



- Relative FCP differences between
  - DoUDP (baseline)
  - DoQ
  - DoH
- At **p40**, FCP increased by <= 10% for DoQ, 20% for DoH
- At **p80**, FCP increased by <= 20% for DoQ, 40% for DoH

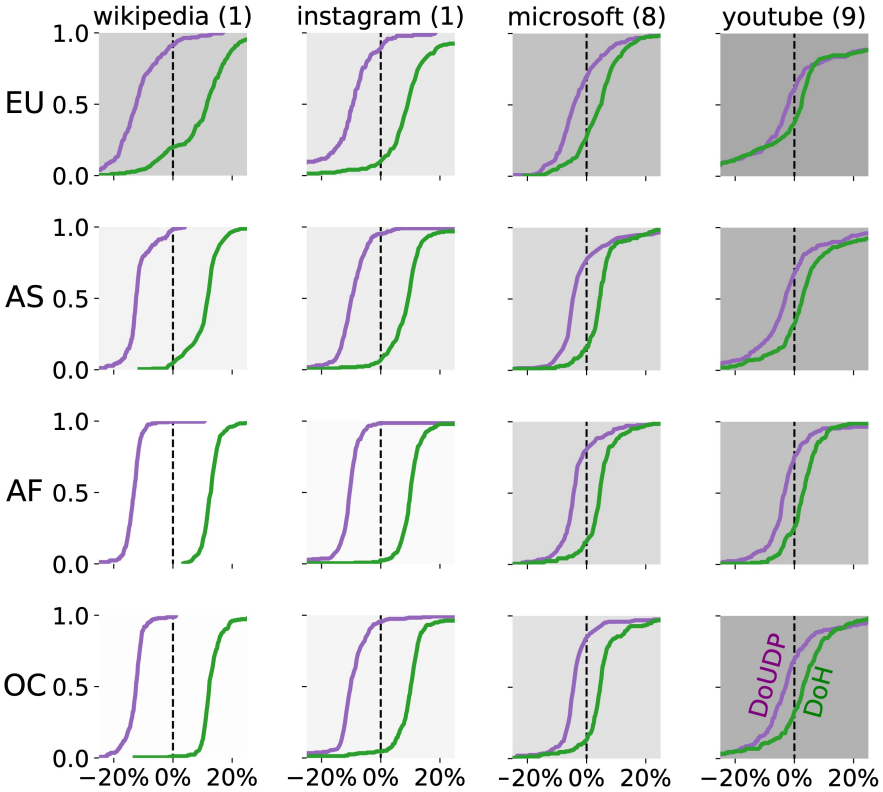
Evaluation – First Contentful Paint over all webpages



- Relative FCP differences between
  - DoUDP (baseline)
  - DoQ
  - DoH
- At **p40**, FCP increased by <= 10% for DoQ, 20% for DoH
- At **p80**, FCP increased by <= 20% for DoQ, 40% for DoH

DoQ significantly improves over DoH

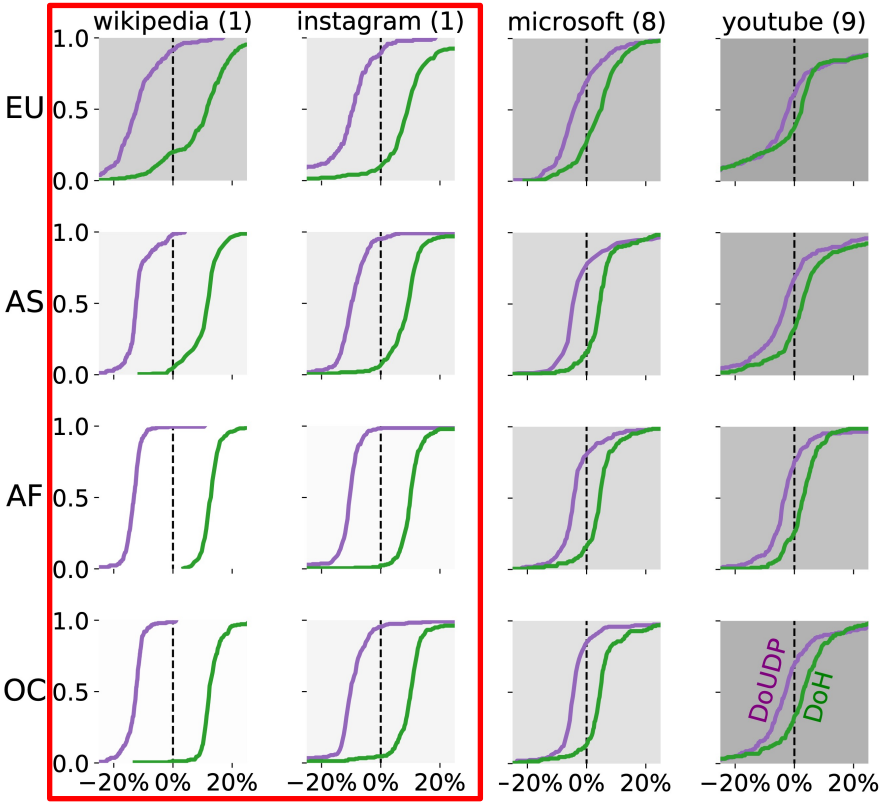
Evaluation – Page Load Time per webpage



- Relative PLT differences between
  - DoQ (baseline)
  - DoUDP
  - DoH

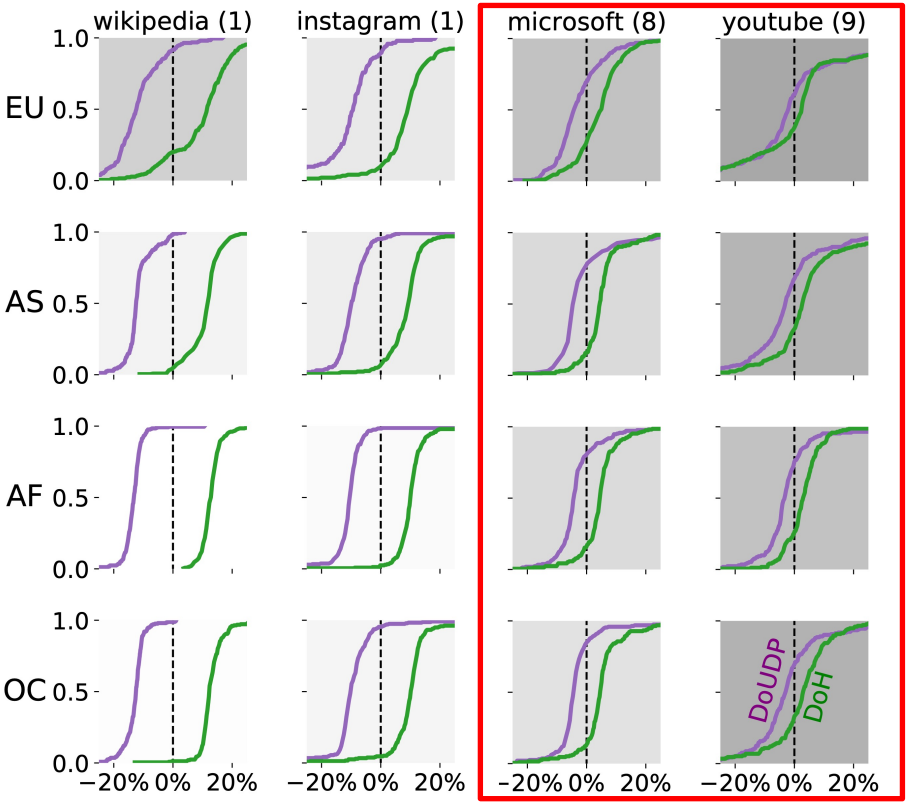
- *Background darkness: helps show trends in larger version of this image in the paper, ignore here*

Evaluation – Page Load Time per webpage



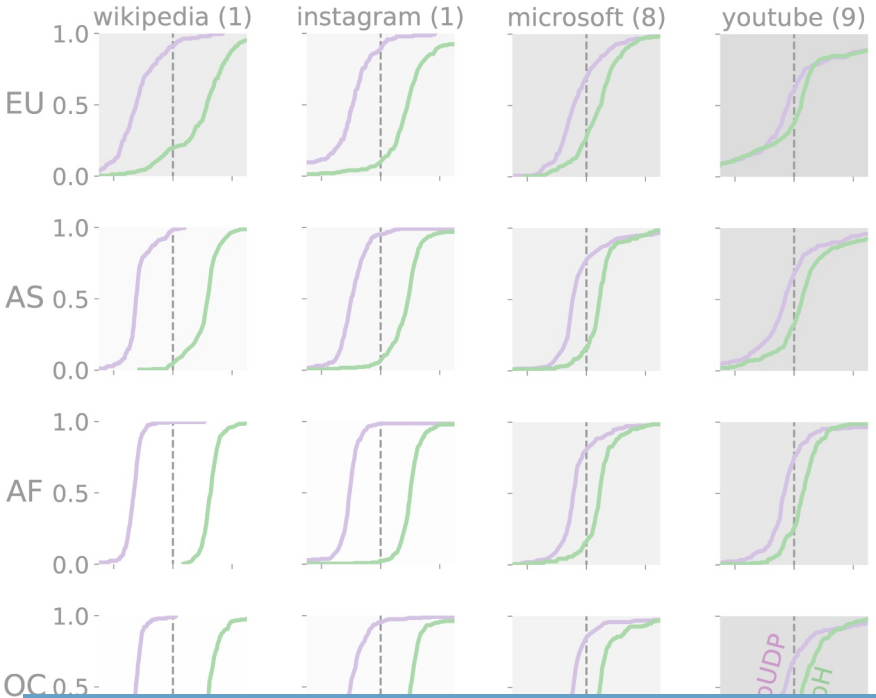
- Simple webpages
  - At p50, DoQ is 10% **faster** than DoH
  - At p50, DoQ is 10% **slower** than DoUDP
  - Cost of encrypted transport is *high*

Evaluation – Page Load Time per webpage



- Complex webpages
  - DoQ, DoH, and DoUDP PLT get closer as the cost of connection setup amortizes the more DNS queries are required
  - **DoQ catches up to DoUDP**
    - 2% difference at p50
  - Cost of encrypted transport is *reduced*

Evaluation – Page Load Time per webpage



- Complex webpages
  - DoQ, DoH, and DoUDP PLT get closer as the cost of connection setup amortizes the more DNS queries are required
  - **DoQ catches up to DoUDP**
    - 2% difference at p50
  - Cost of encrypted transport is *reduced*

DoQ catches up to DoUDP with increasing complexity of webpages

Conclusion

- Encrypted DNS does not have to be a compromise
  - DoQ improves over DoH with up to 10% faster page loads for **simple** webpages
  - DoQ catches up to DoUDP with increasing **complexity** of webpages

  - Caveat: only 10 webpages + 313 resolvers

Conclusion

- Encrypted DNS does not have to be a compromise
  - DoQ improves over DoH with up to 10% faster page loads for **simple** webpages
  - DoQ catches up to DoUDP with increasing **complexity** of webpages
  - Caveat: only 10 webpages + 313 resolvers
- Work is ongoing
  - Unused potential due to missing support for **0-RTT**
  - DNS over HTTPS/3
    - Support recently added by Cloudflare DNS, Google Android* and Public DNS

DoQ makes encrypted DNS much more appealing for the Web

* https://security.googleblog.com/2022/07/dns-over-http3-in-android.html

Paper

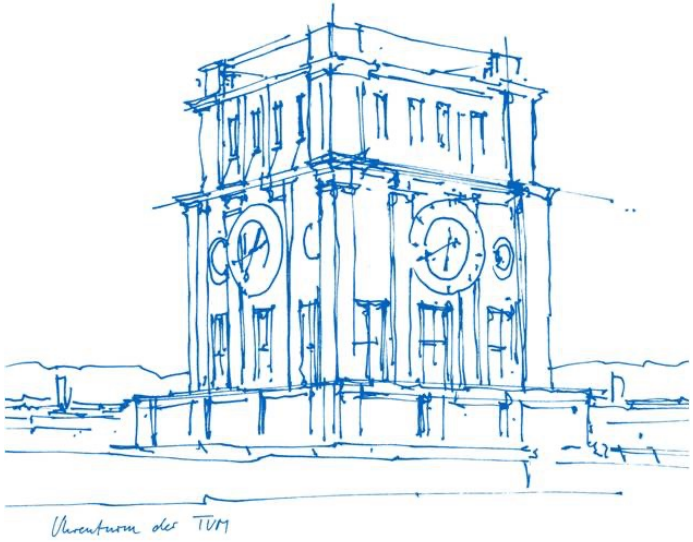
https://bit.ly/3TtqHMV

Code & Dataset

https://bit.ly/3CZ7qME

DoQ makes encrypted DNS much more appealing for the Web

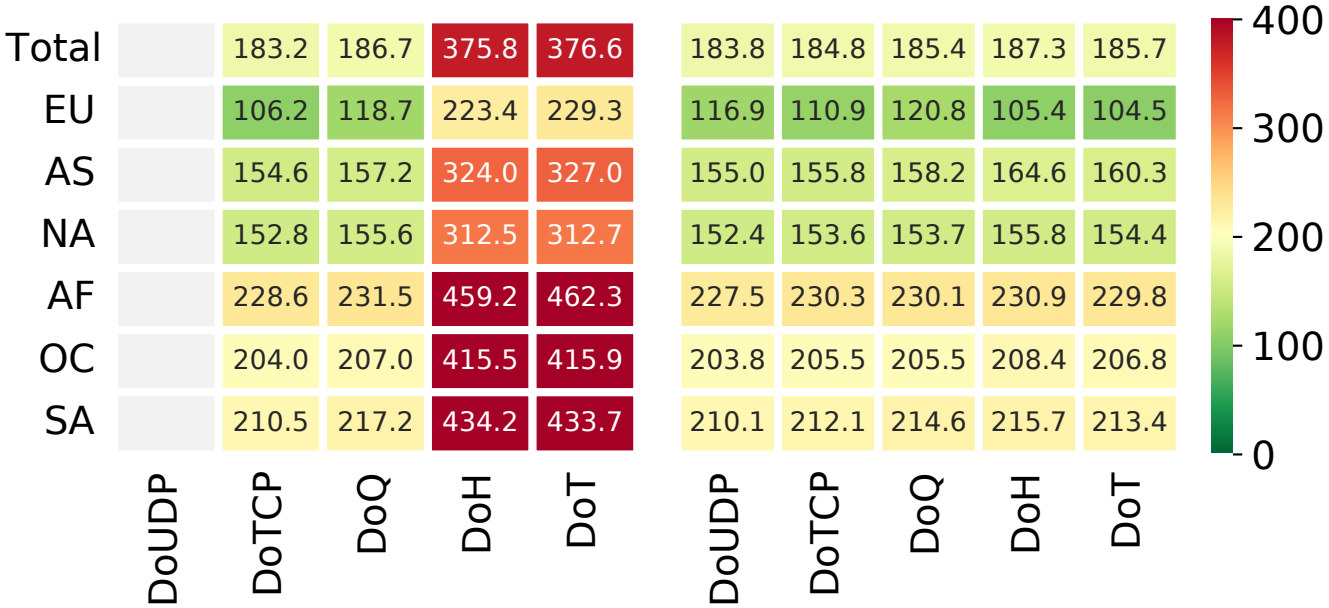
Extra slides



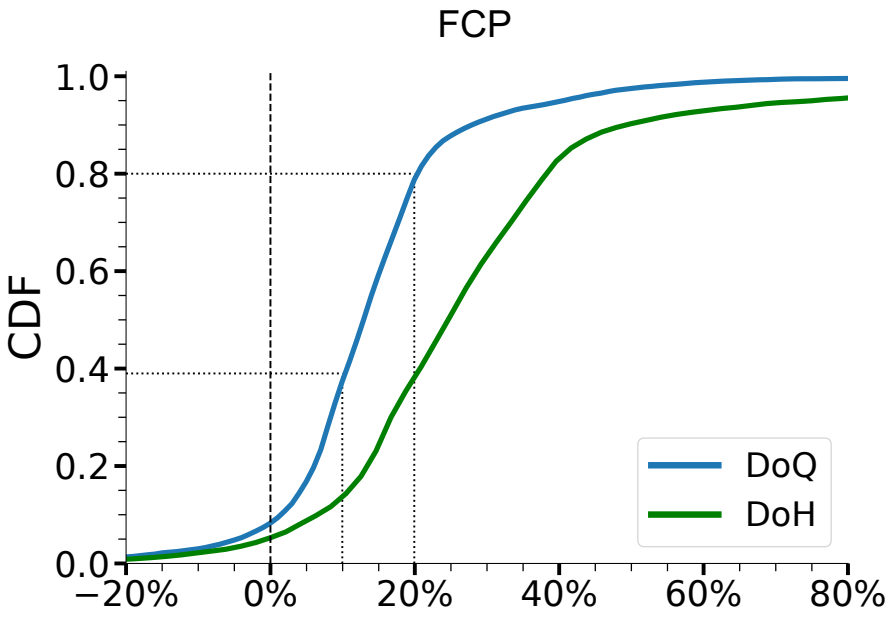
Evaluation – Single Query Sizes

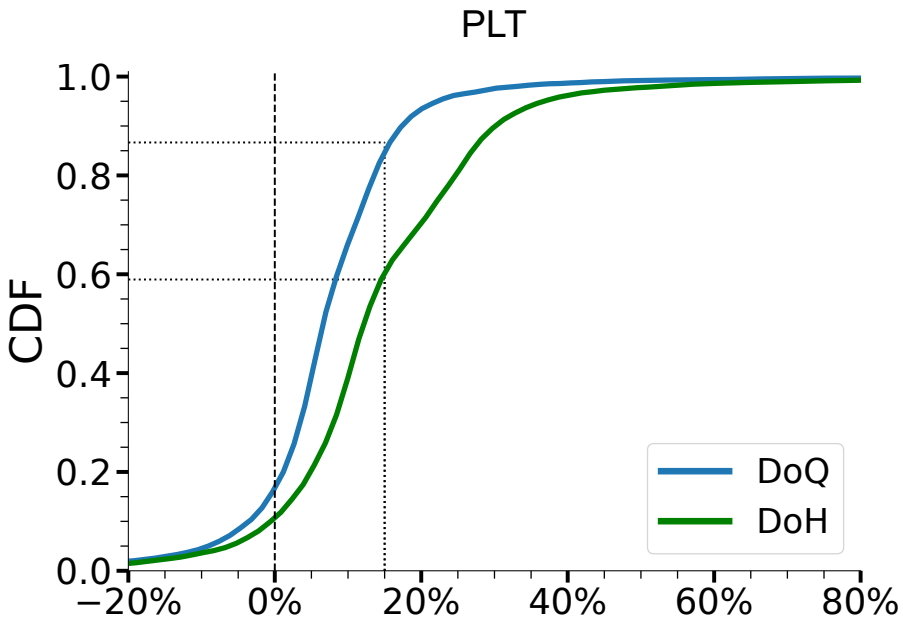
	DoUDP	DoTCP	DoQ	DoH	DoT
Single Query Sizes (median IP payload in bytes)					
— `Total`	122	382	4444	2163	1522
— `Handshake C->R`	—	72	2564	569	551
— `Handshake R->C`	—	40	1304	211	211
— `DNS Query`	59	149	190	579	261
— `DNS Response`	63	121	386	804	499

Evaluation – Response Times



Evaluation – FCP and PLT





14% of DoQ / 41% of DoH measurements
increase the PLT by 15% or more