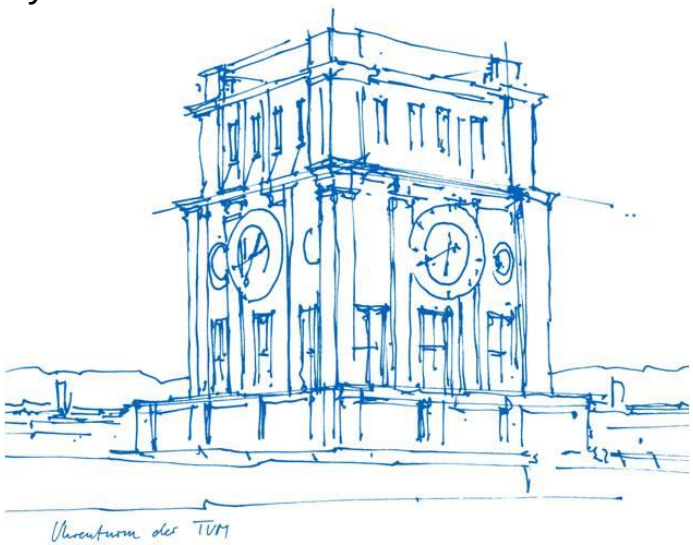
DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance

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

Robin Marx | KU Leuven

Vaibhav Bajpai | CISPA Helmholtz Center for Information Security



Ripe85 2022

Motivation

- Web traffic shifted to HTTPS
- User profiles can be derived by observing unencrypted DNS queries using DNS over UDP (DoUDP)
- Addressed by DNS over TLS (DoT) and DNS over HTTPS (DoH)
- Both are constrained by the round-trips required for the TCP+TLS handshake (2-RTT+)

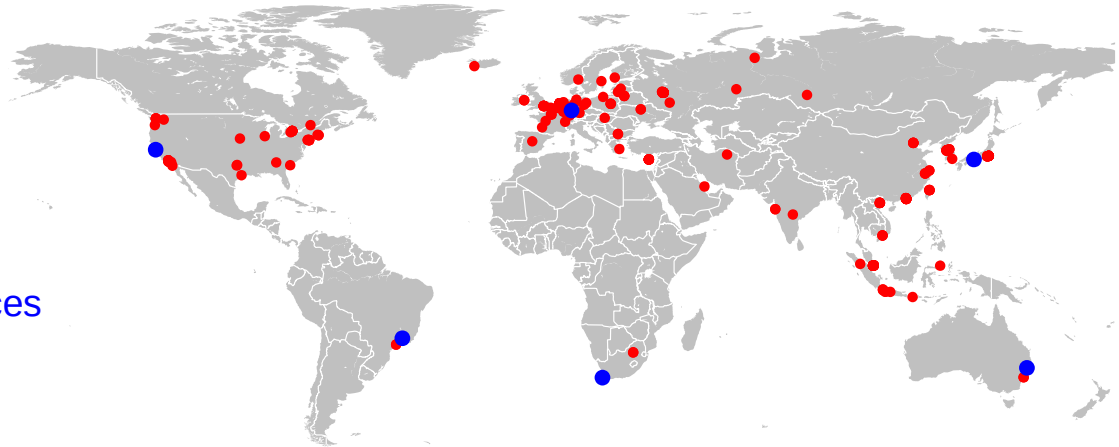
- QUIC combines connection and encryption into 0/1-RTT handshake
- DNS over QUIC (DoQ) aims to provide DNS privacy with minimal latency

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 additionally 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

- 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 navigations: (a) cache warming, and (b) actual Web performance measurement
    - Populate DNS Cache of the resolver
    - QUIC Version negotiation and Address Validation
    - TLS 1.3 Session Ticket

Evaluation – Measurement Overview

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

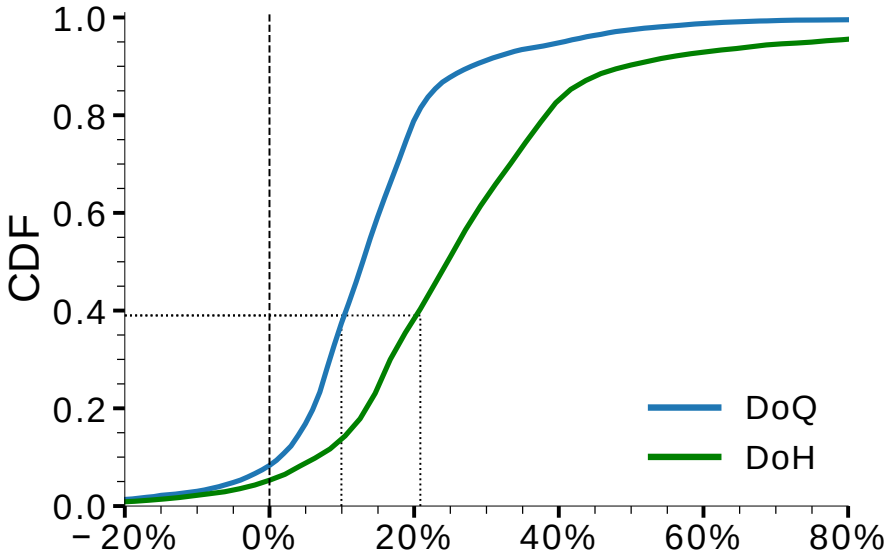
- DNS over QUIC
  - TLS 1.3 Session Resumption 100%
  - 0-RTT 0%
  - QUIC Version *1* *89%*
  - DoQ Draft Version *02* *87%*

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

Evaluation – Metrics

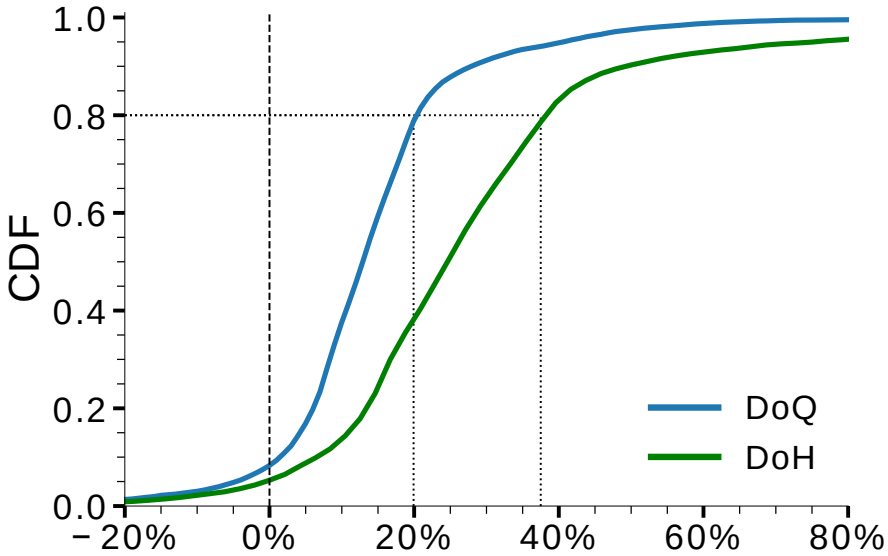
- First Contentful Paint: time until the first visible image or text is shown on the screen
- Page Load Time: time difference between the start of the page load and the onLoad event
- Medians for each **[vantage point:resolver:DNS protocol]** combination to account for geographical distances between VP and resolvers
- Compare the per-protocol medians corresponding to a pair of **[vantage point:resolver]**

Evaluation – First Contentful Paint over all webpages



- Relative FCP differences between
  - DoUDP (baseline)
  - DoQ
  - DoH
- 40% of DoQ measurements increase the FCP by 10% or less, DoH by 20%

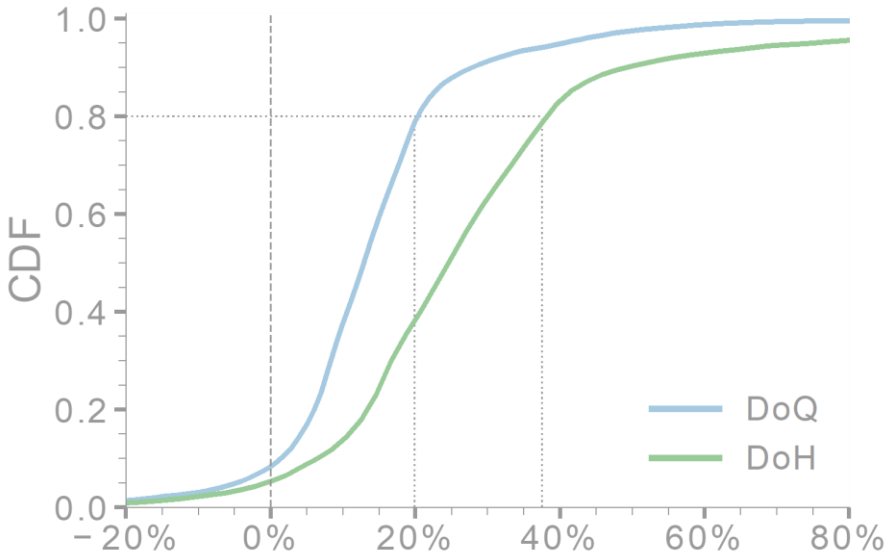
Evaluation – First Contentful Paint over all webpages



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

- 40% of DoQ measurements increase the FCP by 10% or less, DoH by 20%
- 20% of DoQ measurements increase the FCP by 20% or more, DoH by 40%

Evaluation – First Contentful Paint over all webpages

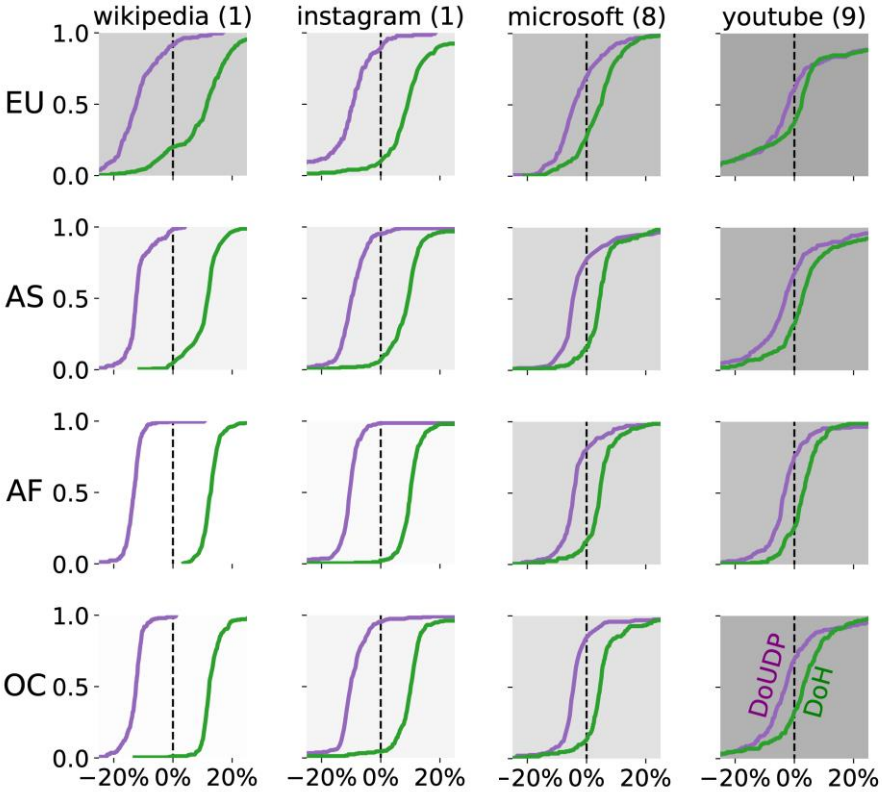


- Relative FCP differences between
  - DoUDP (baseline)
  - DoQ
  - DoH

- 40% of DoQ measurements increase the FCP by 10% or less, DoH by 20%
- 20% of DoQ measurements increase the FCP by 20% or more, DoH by 40%
- 10% of DoQ and DoH measurement decrease the FCP

DoQ significantly improves over DoH

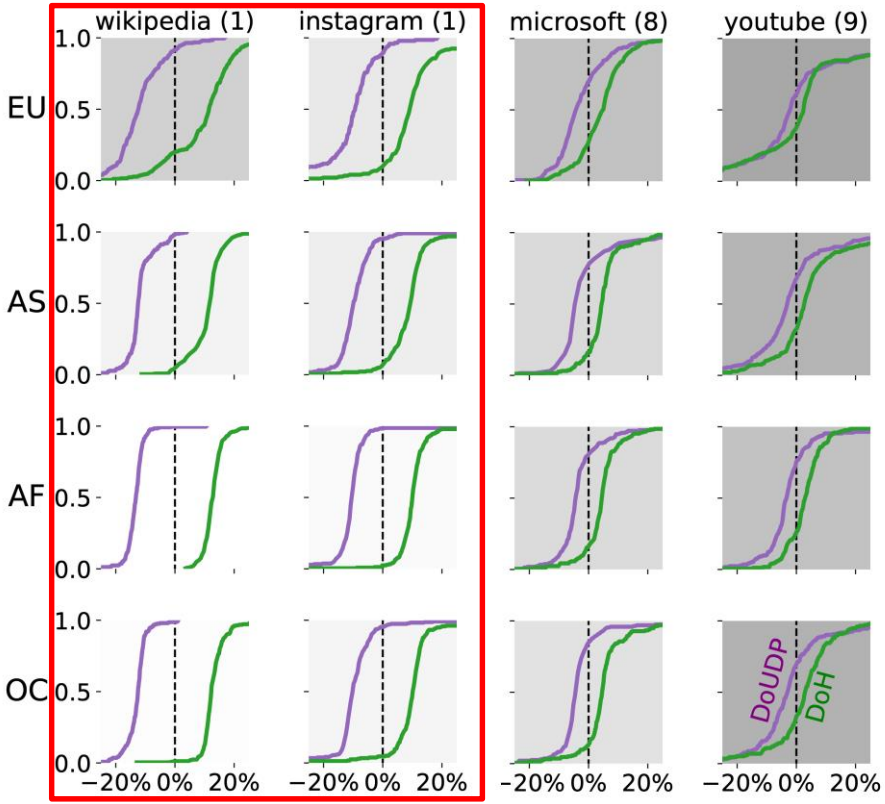
Evaluation – Page Load Time per webpage



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

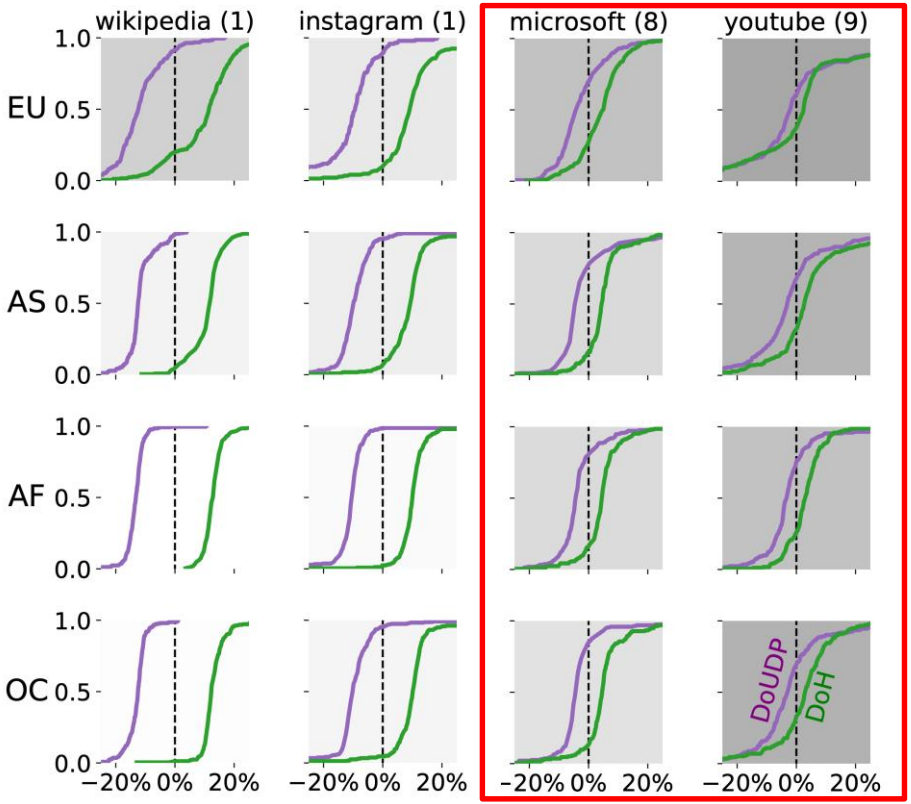
- Lighter background color: a higher percentage of DoQ Page Loads are faster than DoH
- Improvements diminish the more DNS queries are required for loading a webpage (darker color)

Evaluation – Page Load Time per webpage



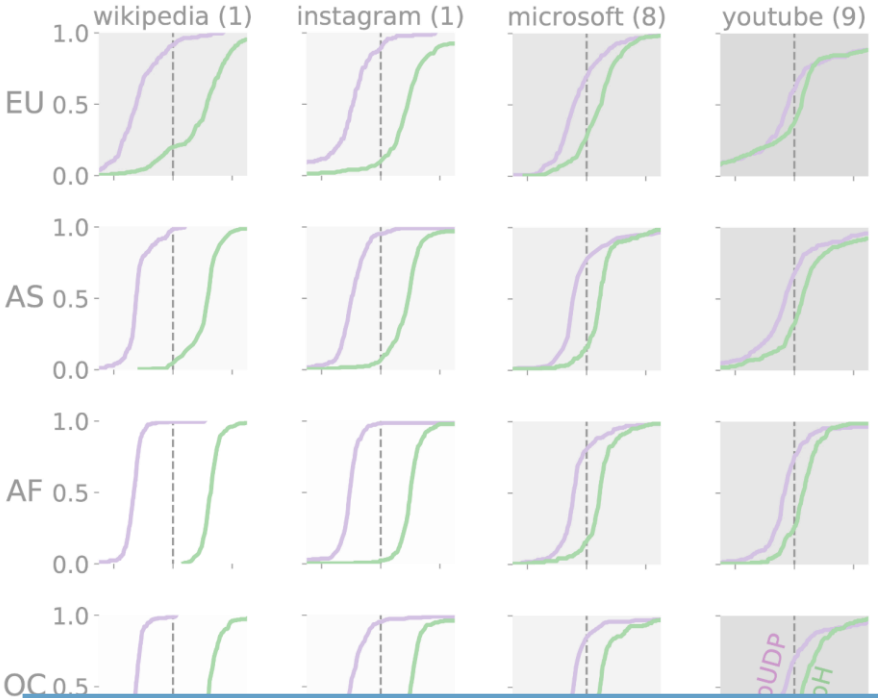
- Simple webpages
  - DoQ improves the PLT over DoH by up to 10% in the median
  - DoQ worsens the PLT over DoUDP by up to 10% in the median
  - Cost of encryption is the largest

Evaluation – Page Load Time per webpage



- Complex webpages
  - DoQ, DoH, and DoUDP PLT get closer as the cost of encryption amortizes the more DNS queries are required
  - DoQ catches up to DoUDP
  - Cost of encryption is the smallest

Evaluation – Page Load Time per webpage



- Complex webpages
  - DoQ, DoH, and DoUDP PLT get closer as the cost of encryption amortizes the more DNS queries are required
  - DoQ catches up to DoUDP
  - Cost of encryption is the smallest

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
  - 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

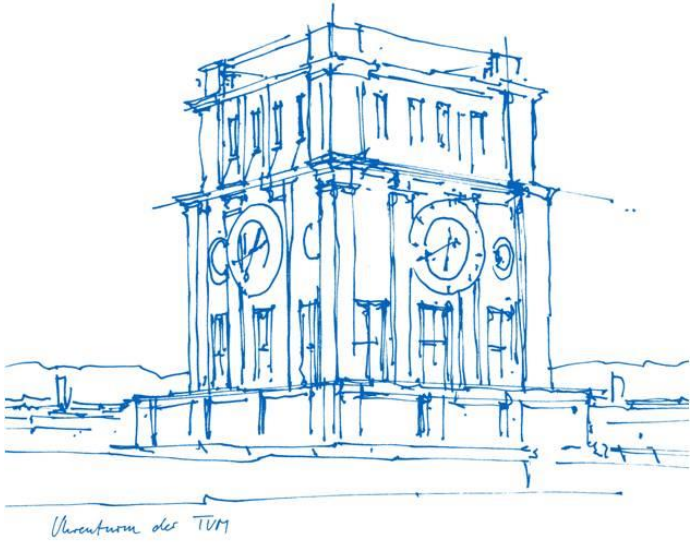
Paper

https://bit.ly/3TtqHMV

Code & Dataset

https://bit.ly/3CZ7qME

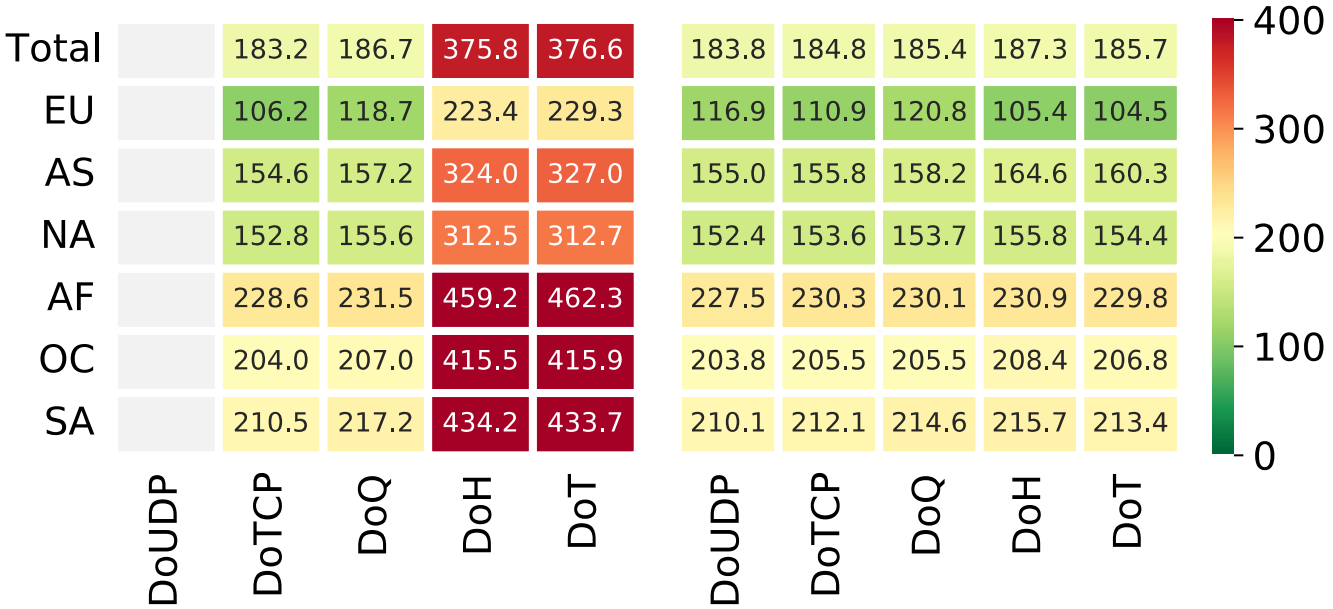
DoQ makes encrypted DNS much more appealing for the Web


Uhrenturm der TUM

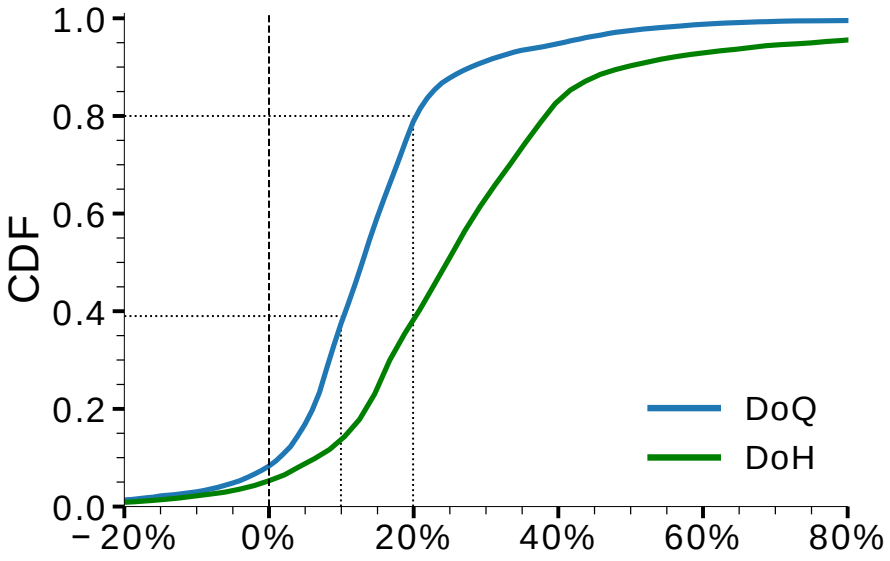
Evaluation – Single Query Sizes

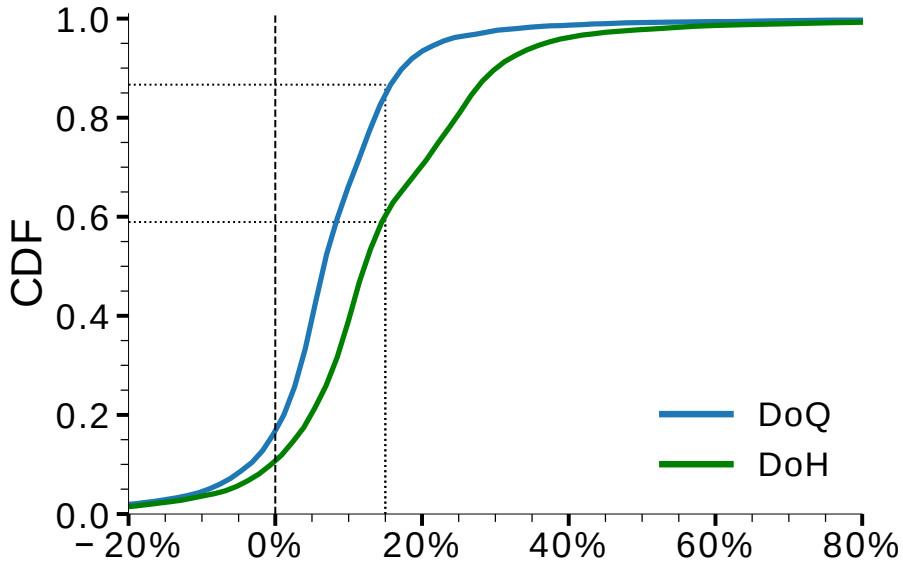
	DoUDP	DoTCP	DoQ	DoH	DoT
Single Query Sizes (median IP payload in bytes)					
— Total	122	382	4444	2163	1522
— Handshake C->R	—	72	2564	569	551
— Handshake R->C	—	40	1304	211	211
— DNS Query	59	149	190	579	261
— DNS Response	63	121	386	804	499

Evaluation – Response Times



Evaluation – FCP and PLT





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