One to Rule them All? A First Look at DNS over QUIC

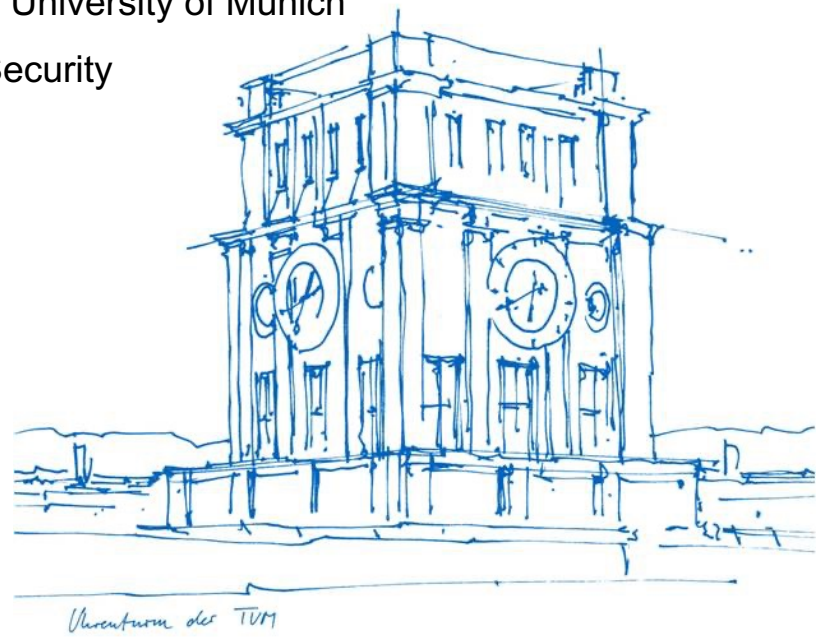
Mike Kosek, Trinh Viet Doan, Malte Granderath | Technical University of Munich

Vaibhav Bajpai | CISPA Helmholtz Center for Information Security

IETF 113 Vienna/Virtual | maprg

Accepted at PAM 2022

23.03.2022



DNS over QUIC (DoQ)

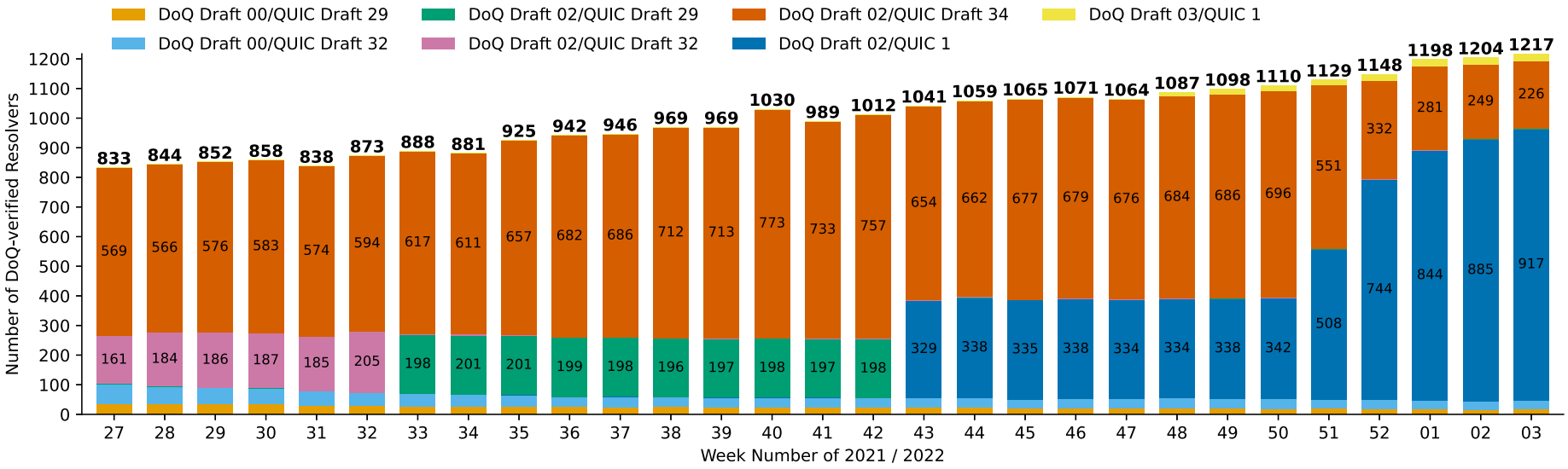
- Final standardization stage
- Combines connection and encryption into 0/1-RTT handshake
- Experimental implementations exist for Clients and Servers
- Used in production systems (e.g., `AdGuard`, `nextDNS`)
- No studies focusing on DoQ exist to date

- One to Rule them All? A First Look at DNS over QUIC
  - Adoption
  - Response Times

Adoption – Methodology

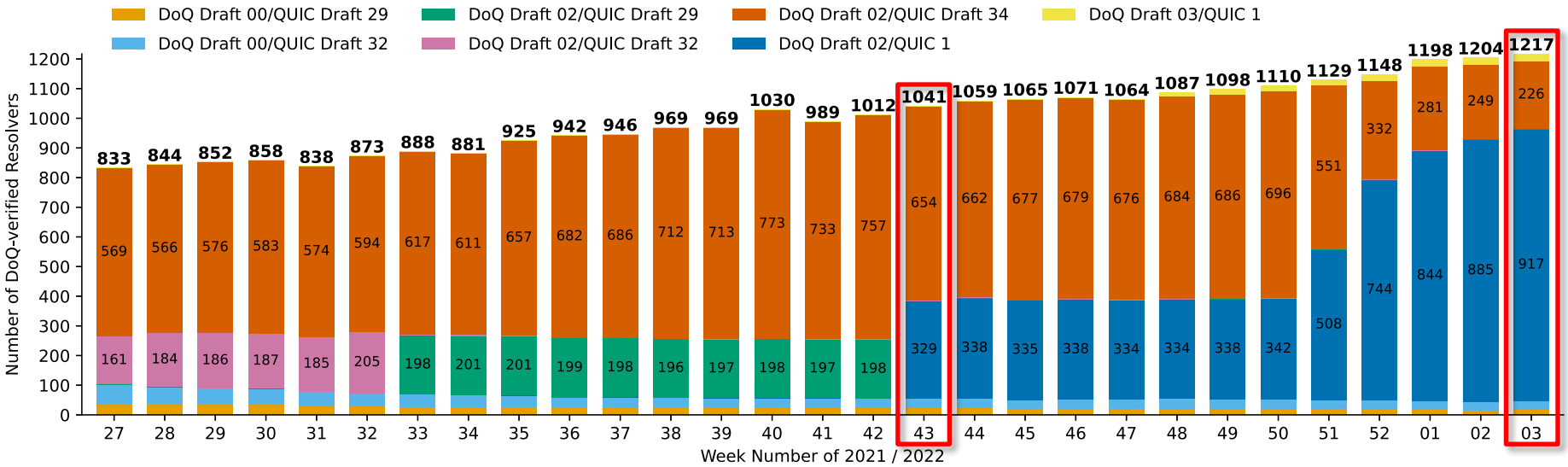
- Weekly scans over 29 Weeks of the IPv4 address space from a single vantage point at TUM
- DNS over UDP (DoUDP) as a baseline
- DNS over QUIC
  - DoQ versions: in the order of draft-06 to draft-00
  - QUIC versions 1, draft-34, -32, and -29
- Metrics
  - Negotiated DoQ and QUIC versions
  - Common Names of X.509 Certificates

Adoption – Findings



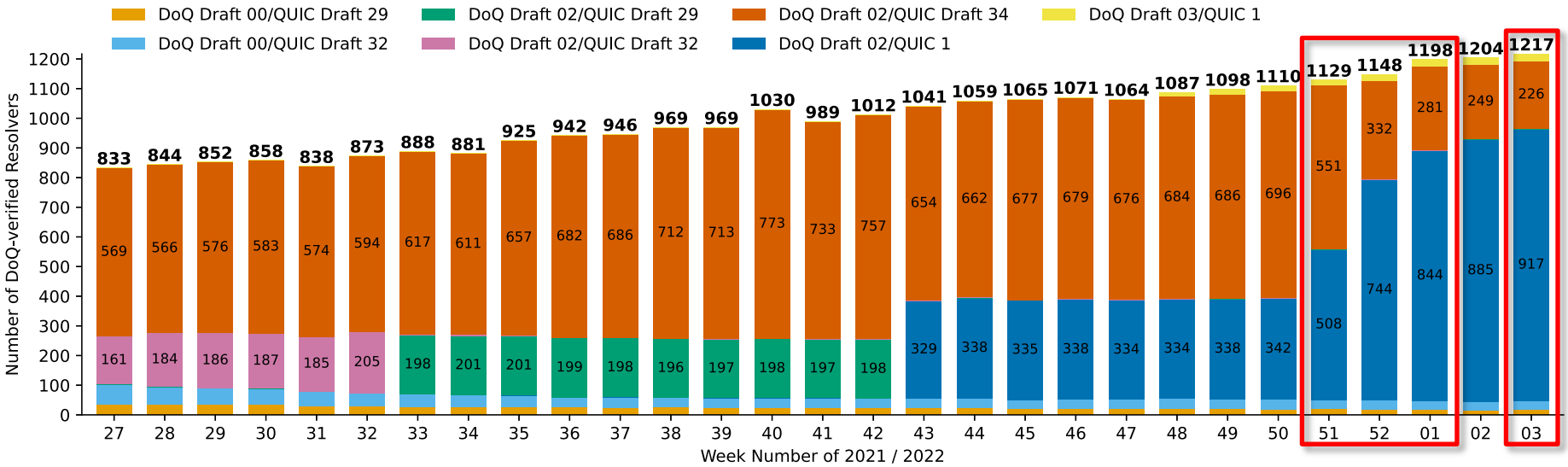
- Adoption rises slow but steadily: increase by ~46% to 1217 Resolvers
- High fluctuation: ~52% of W27 resolvers are still reachable in W03
- DoUDP: ~292m resolvers, ~97% of W27 resolvers are still reachable in W03

Adoption – Findings



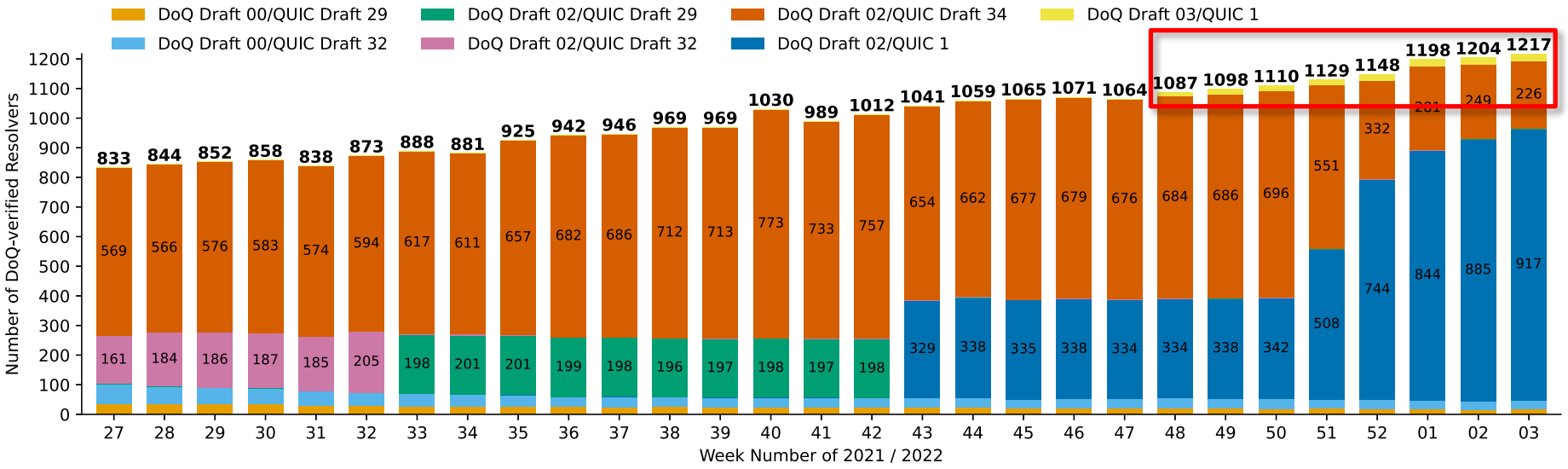
- We observe only 7 DoQ/QUIC version pairs
- Added support for QUIC 1 in W43
- Dominated by DoQ Draft 02/QUIC 1 (dark blue bars) in W03

Adoption – Findings



- Uptake of DoQ Draft 02/QUIC1 in W51-W01
- Open source DNS Server implementation *AdGuard Home*
  - Changed from QUIC Draft 34 to QUIC 1 | Verified by Common Names (e.g., *adguard.llli.live*)

Adoption – Findings



- *AdGuard:* ~25 resolvers in W03, Common Names *dns.adguard.com, adguard.ch*

Response Times – Methodology

- Hourly measurements over the course of W03/2022 from a single vantage point at TUM
  - Using list of IPv4 addresses from adoption scan as measurement targets
  - Single Query per protocol
  - Location Bias

- Measurement of DoUDP, DoTCP, DoT, DoH, and DoQ
  - 264 Verified Resolvers which support *all* targeted DNS protocols
  - 2 subsequent queries: Cache-warming and actual measurement

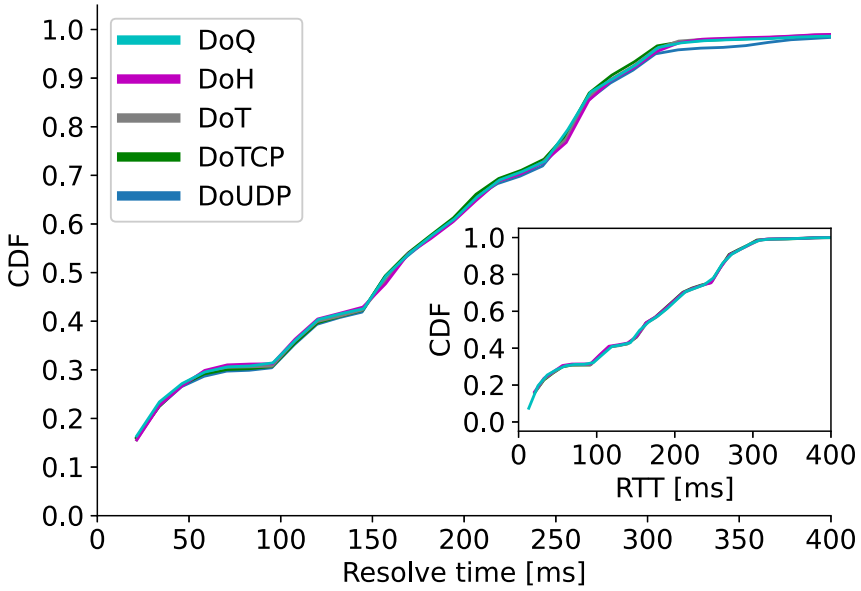
- Metrics
  - Handshake Time
  - Resolve Time

  } sum of both = total time to lookup a name (i.e., Response Time)

  - Protocol-specific RTT
  - Limitations: We do not support TLS Session Resumption and Early Data (0-RTT)

Response Times – Findings

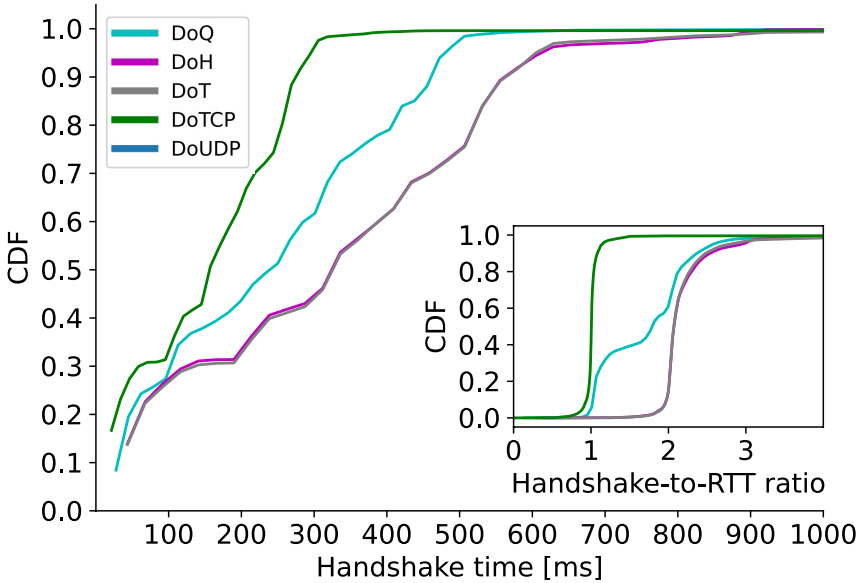
- Expectation for Resolve Time and RTT
  - All protocols: 1 RTT ✓
- Findings for all protocols
  - Resolve Times are identical
  - No protocol specific path influences
  - Resolve Times and RTTs are identical



Response Times – Findings

- Expectation for Handshake Time
  - DoTCP: 1 RTT ✓
  - DoT/DoH: 2 RTTs (TLS 1.3) (✓)
  - DoQ: 1 RTT X

- Findings for DoQ
  - Falls short of DoTCP, improves on DoT/DoH
  - 20% 1 RTT | 40% 1-2 RTTs | 40% > 2 RTTs



Response Times – Analysis

- *QUIC* `Client Address Validation`*: Prevent traffic amplification attacks*
- We reuse the `TOKEN` issued in the cache-warming query in the subsequent `INITIAL`
- `Client Address Validation` is fulfilled

- However, handshake is still limited by the *traffic amplification limit*
  - Server stops sending if 3x the amount of data received by the client is reached
  - Depending on the X.509 Certificate size, the Cert fits into this limit, or exceeds it
  - If it fits: +0 RTT
  - If not: +1 RTT

Not specific to DoQ, but a QUIC implementation Bug

Conclusion

- Adoption
  - Rises slowly with High Week-over-week fluctuations

- Response Times
  - QUIC's potential is fully utilized in ~20% of measurements
  - ~40% of measurements show considerably higher handshake times than expected
  - Still unused optimization potential, but DoQ already outperforms DoT as well as DoH

DoQ already is the best choice for encrypted DNS to date

Paper

Code & Dataset