5TH NIST PQC STANDARDIZATION CONFERENCE

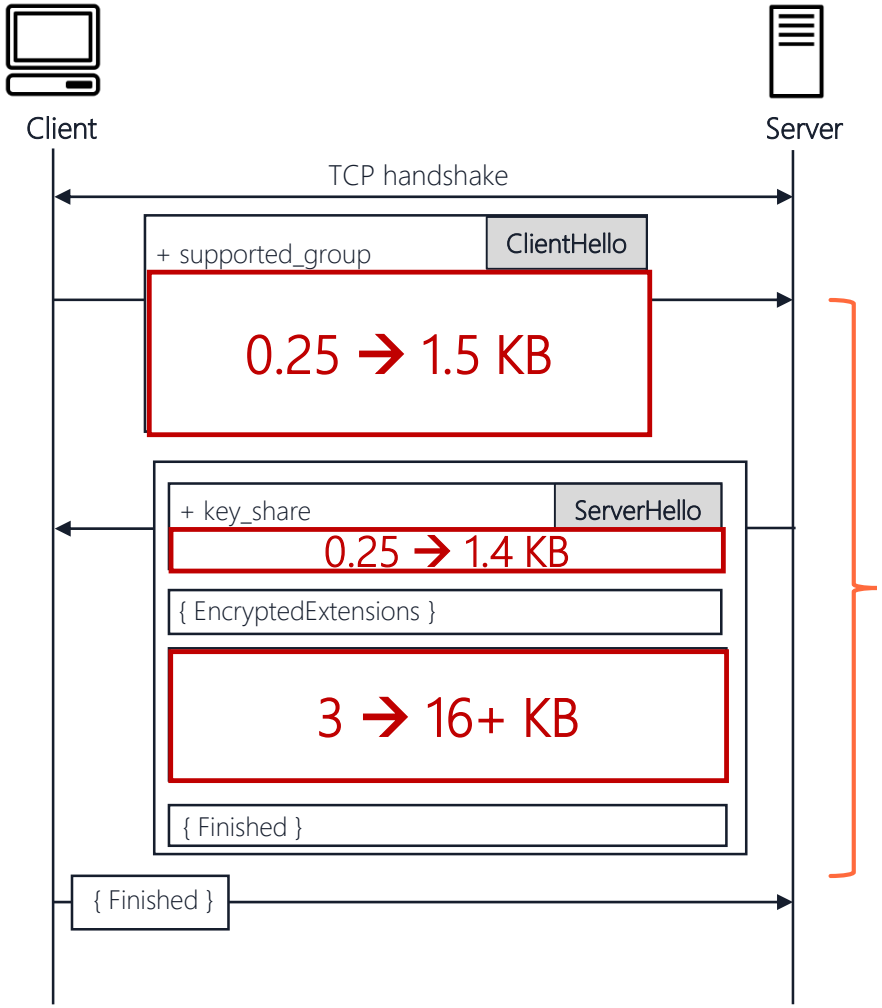
The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections

[ia.cr/2024/176]

Panos Kampanakis, Will Childs-Klein

AWS

Why? - TLS 1.3 handshake



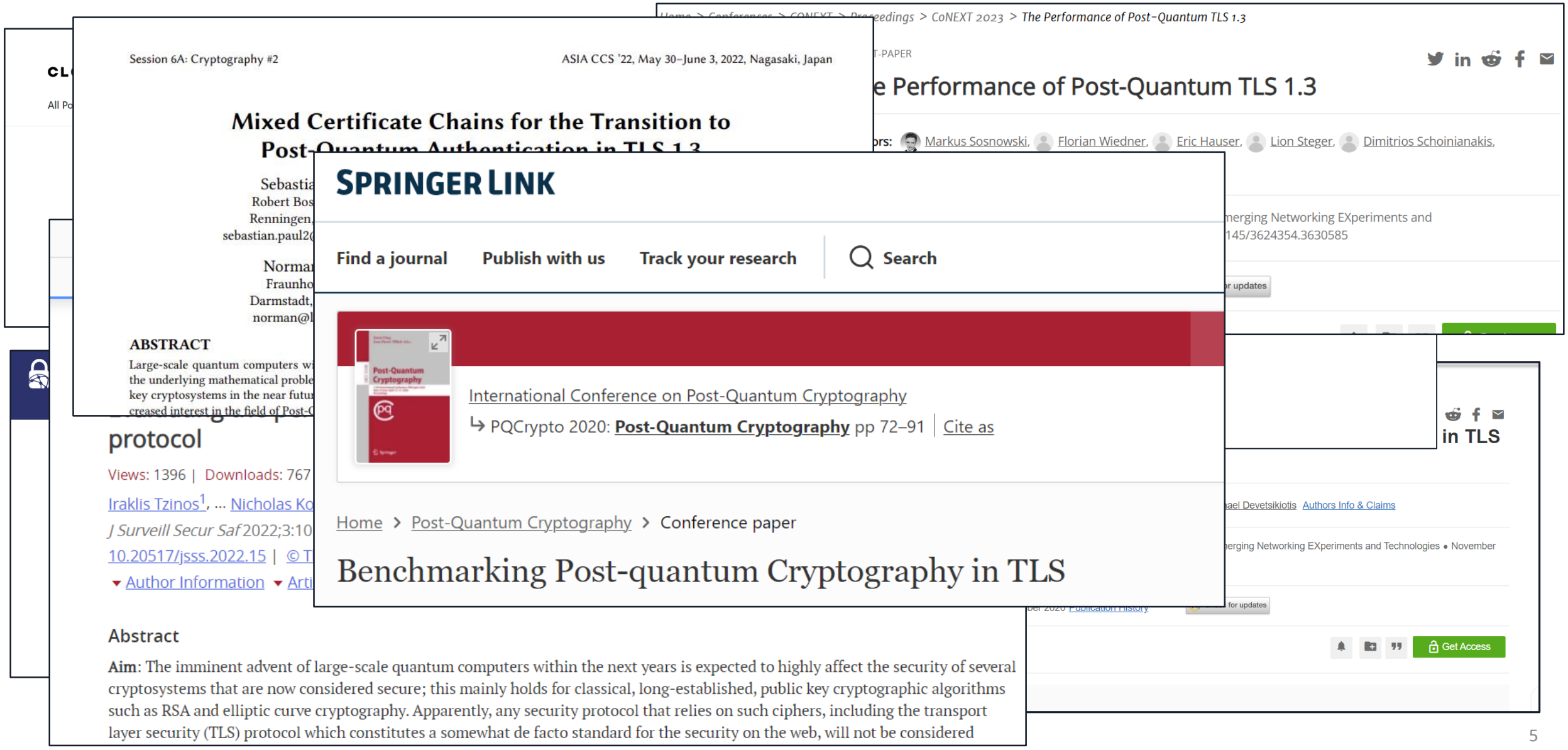
1 Round-Trip (RTT)

1 RTT

If the PQ ephemeral public key and certs introduce an extra x ms, the handshake % increase is H=**x/2RTT**.

(@ 1Mbps, 15 extra KB → x=120ms
(@ 1Gbps, 15 extra KB → x=0.12ms)

PQ TLS Handshake Studies



TLS 1.3 Handshake Time

Great metric for

- Algorithm vs Algorithm in TLS 1.3 performance comparison

Good indicator of

- Time-To-First-Byte (TTFB) Performance

But what does it mean about application performance

- 30% PQ TLS 1.3 handshake slowdown ≈ 30% application slowdown
- 25% PQ TLS 1.3 handshake slowdown ≈ 25% slower browser experience

What is perceived performance?

Google PageSpeed Insights

- First Contentful Paint (FCP)
- Largest Contentful Paint (LCP)

} Loading page content

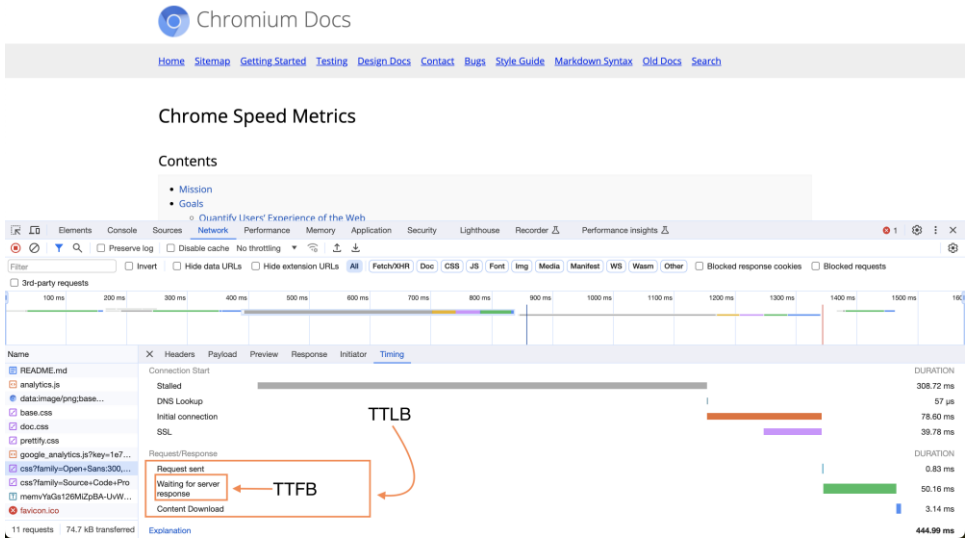
- (Experimental) Time to First Byte (TTFB)

} DNS redirect + TLS + Redirect time + request-response

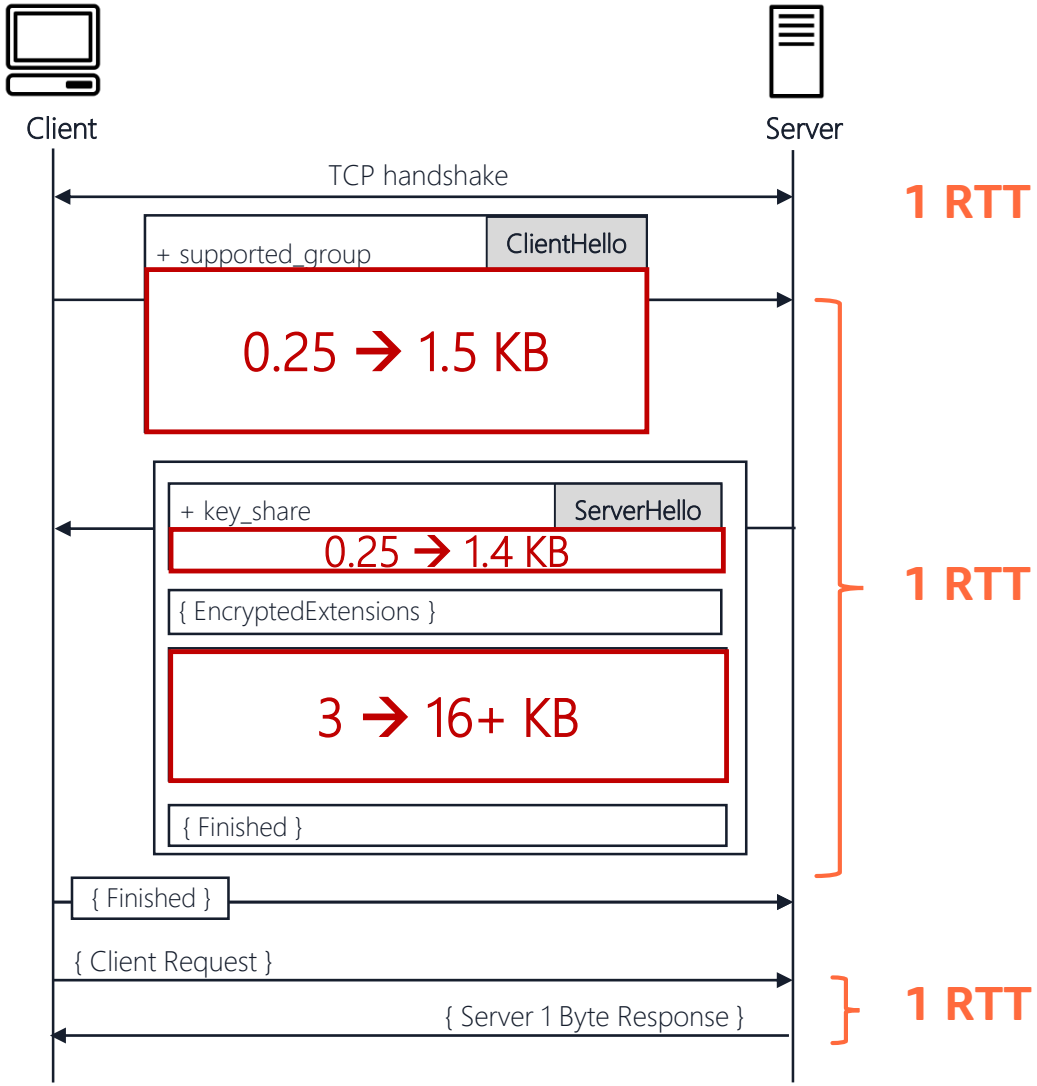
- Cumulative Layout Shift (CLS)
- Interaction to Next Paint (INP)

} After page is loaded

Other Applications



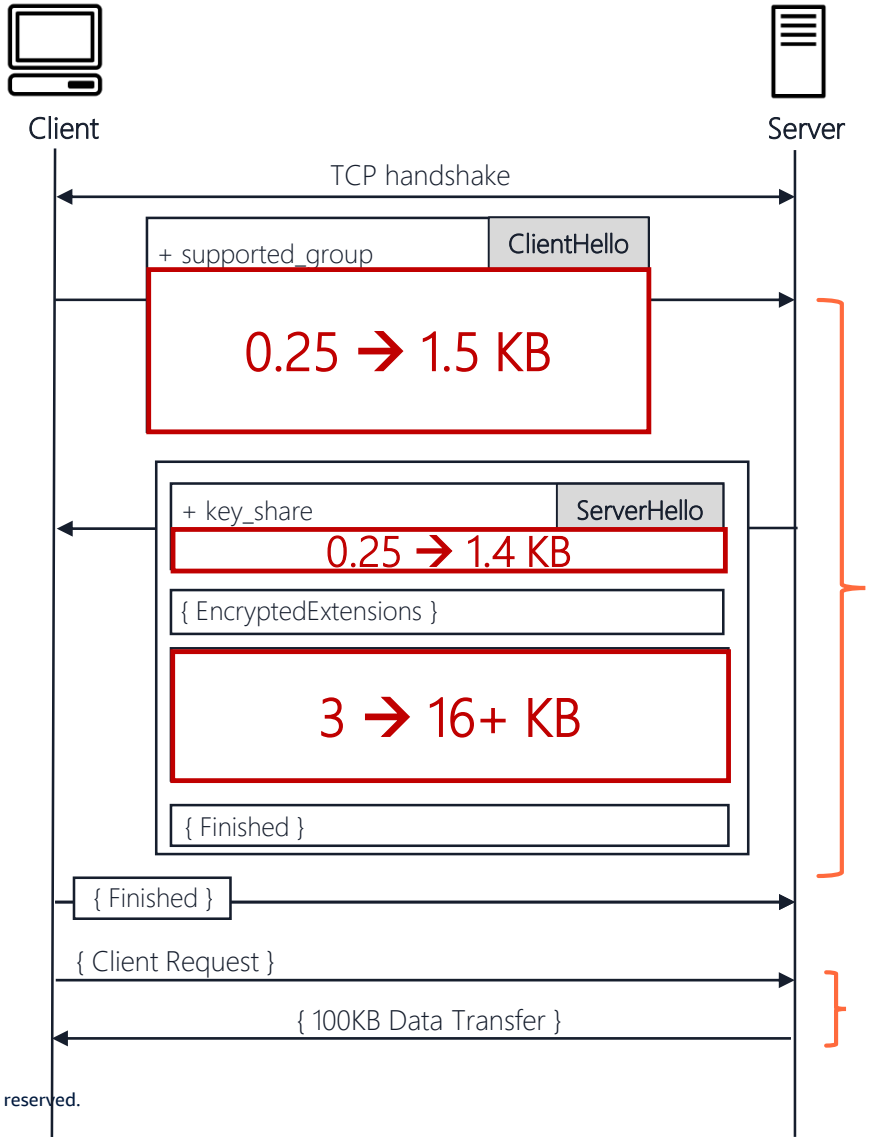
Why? - TLS 1.3 handshake vs TTFB



If the PQ ephemeral public key and certs introduce an extra x ms, the handshake % increase is H=x/2RTT.

The TTFB % increase is x/3RTT **(=0.66*H)**.

Why? - TLS 1.3 handshake vs TTFB vs TTLB



1 RTT

1 RTT

3 RTTs

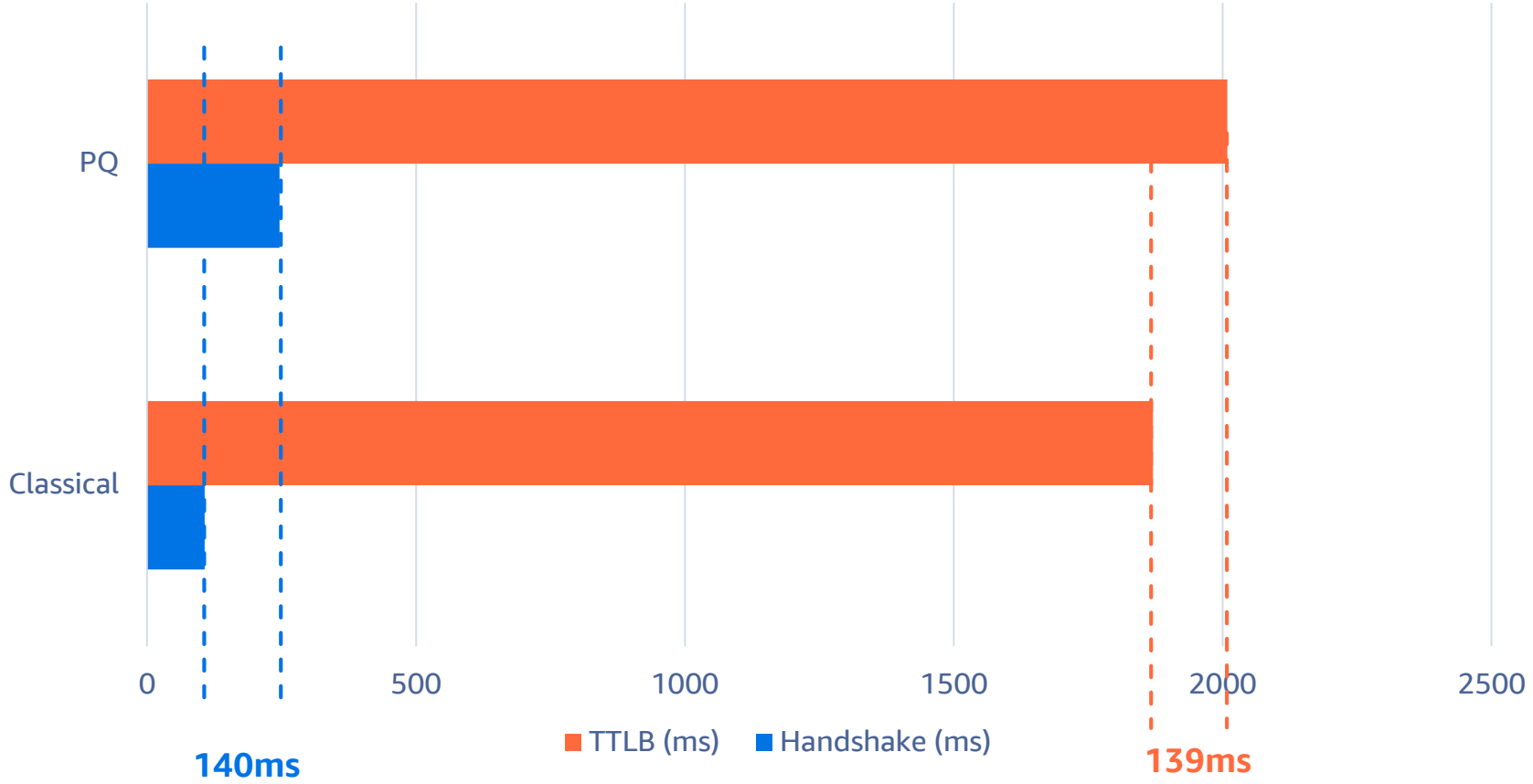
If the PQ ephemeral public key and certs introduce an extra x ms, the handshake % increase is H=x/2RTT.

The TTFB % increase is x/3RTT (=0.66*H).

The TTLB % increase is x/5RTT **(=0.40*H)**.

Why Time-To-Last-Byte?

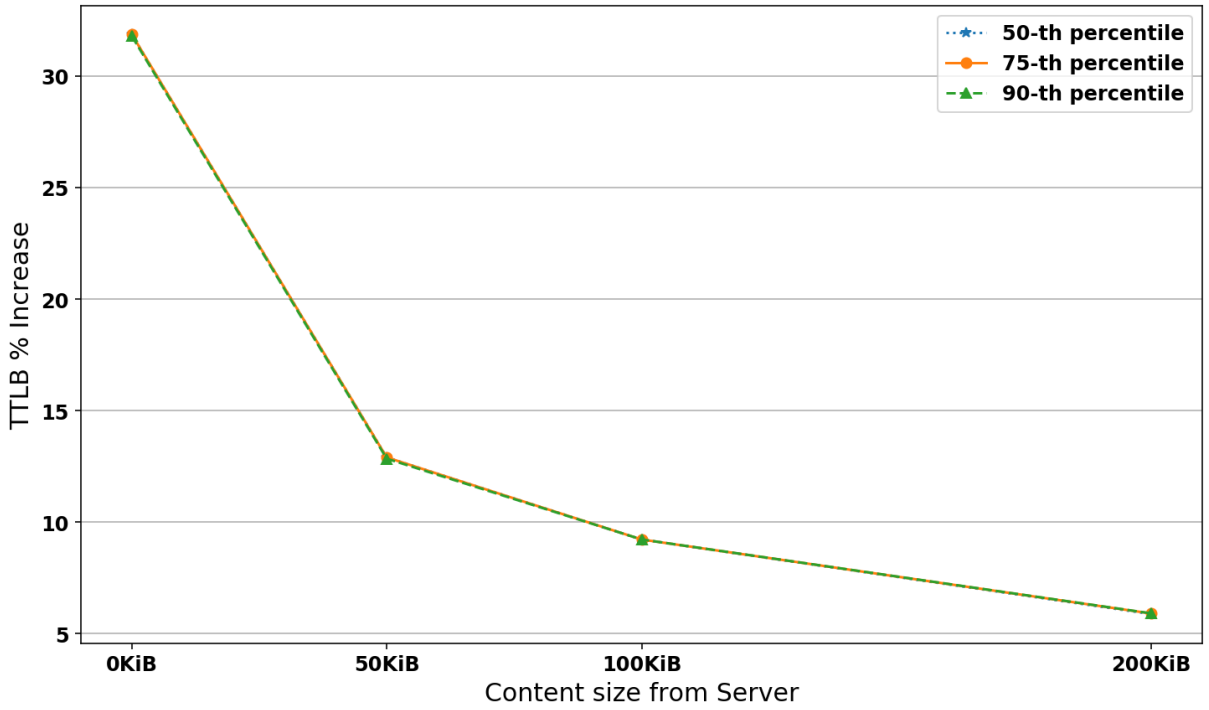
200 KIB TRANSFER, 1 MBPS, 0% LOSS, 35MS RTT, INITCWND=20MSS



TTLB % increase

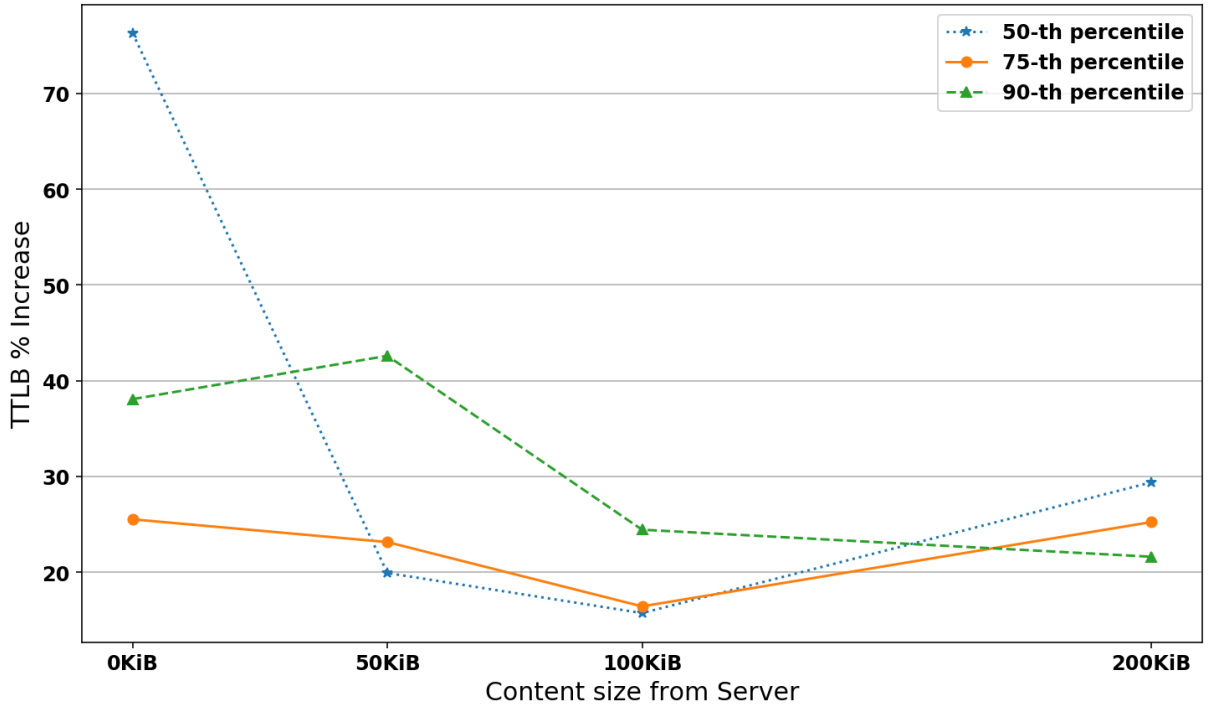
1MBPS, 200MS RTT, INITCWND=20MSS

0% loss



The classical connection TTLB percentiles at 200KiB are 2.3 seconds

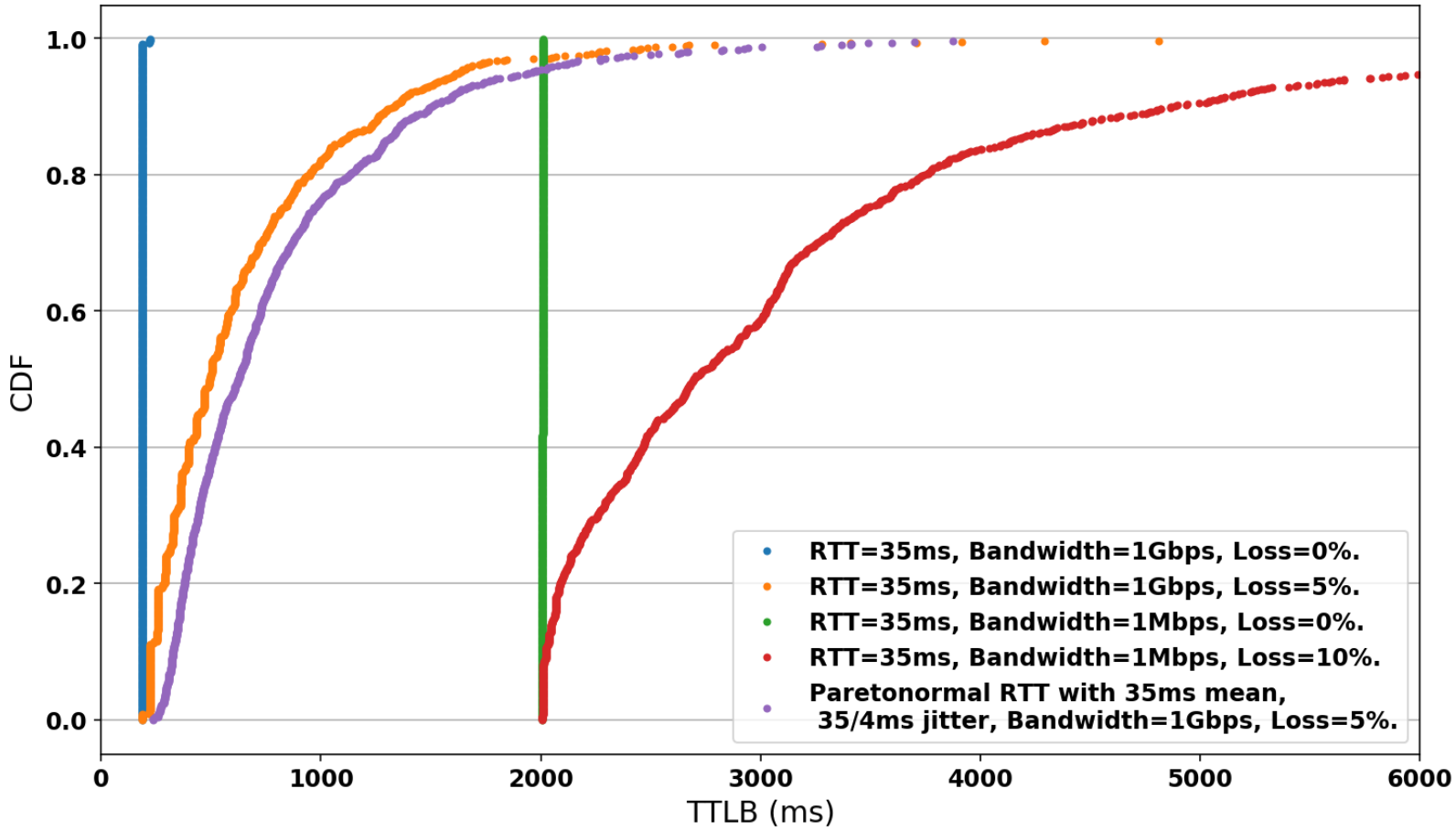
10% loss



The classical connection TTLB percentiles at 200KiB are [4.6, 7.1, 10.1] seconds

Cumulative Distribution Function (CDF)

PQ TTLB CDF, 200 KIB TRANSFER, 35MS RTT, INITCWND=20MSS
(CLASSICAL TTLBS WERE SIMILAR)



Takeaways

1. TTLB may be a better application performance indicator.
2. Handshake impact may overestimate the effect on the connection by y/(y+2) %
3. PQ impact on TTLB drops as data transfer size increases
   - <20% for >50KB of data
4. Low bandwidth connections see more impact from PQ
   - The impact is less significant for sizable data transfers
5. Network instability affects classical and PQ connections similarly.

6. But yes, let’s still find ways to alleviate the PQ handshakes.

Thank you!

Panos Kampanakis

kpanos@amazon.com

Will Childs-Klein

childw@amazon.com