



5TH NIST PQC STANDARDIZATION CONFERENCE

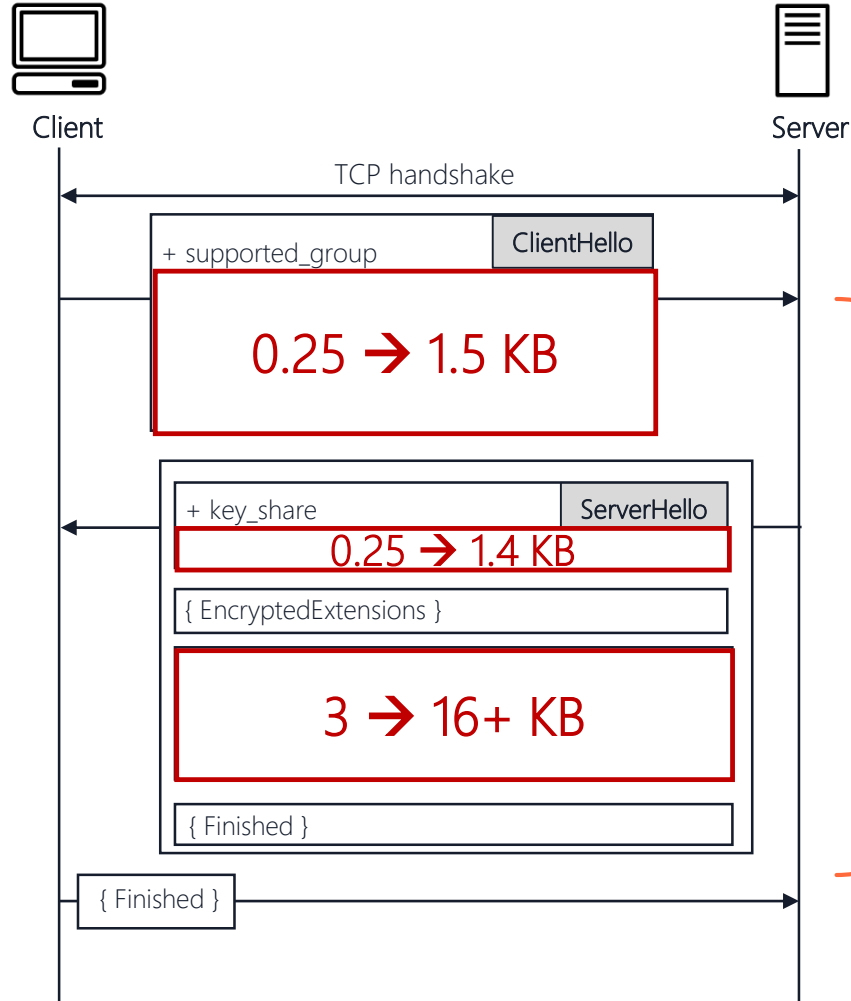
# The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections

[\[ia.cr/2024/176\]](https://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 →  $x=120$ ms  
(@ 1Gbps, 15 extra KB →  $x=0.12$ ms)

# PQ TLS Handshake Studies

Session 6A: Cryptography #2 ASIA CCS '22, May 30–June 3, 2022, Nagasaki, Japan

## Mixed Certificate Chains for the Transition to Post-Quantum Authentication in TLS 1.3

Sebastian Paul, Robert Bos, Renning, sebastian.paul2022@uni-darmstadt.de

Normal Fraunhofer Darmstadt, norman@fhnw.ch

ABSTRACT  
Large-scale quantum computers will affect the underlying mathematical problems of many key cryptosystems in the near future. This has increased interest in the field of Post-Quantum Cryptography (PQC) and its integration into the TLS protocol.

Views: 1396 | Downloads: 767

Iraklis Tzinos<sup>1</sup>, ... Nicholas Kourtellis<sup>2</sup>, ...  
*J Surveill Secur Saf* 2022;3:10  
10.20517/jsss.2022.15 | © Tzinos et al. 2022  
Author Information | Article Information

Abstract  
**Aim:** The imminent advent of large-scale quantum computers within the next years is expected to highly affect the security of several cryptosystems that are now considered secure; this mainly holds for classical, long-established, public key cryptographic algorithms such as RSA and elliptic curve cryptography. Apparently, any security protocol that relies on such ciphers, including the transport layer security (TLS) protocol which constitutes a somewhat de facto standard for the security on the web, will not be considered

Home > Conferences > CoNEXT > Proceedings > CoNEXT 2023 > The Performance of Post-Quantum TLS 1.3

## The Performance of Post-Quantum TLS 1.3

Authors: Markus Sosnowski, Florian Wiedner, Eric Hauser, Lion Steger, Dimitrios Schoiniarakis

Emerging Networking Experiments and Technologies • November 2022  
145/3624354.3630585

for updates

in TLS

Home > Post-Quantum Cryptography > Conference paper

## Benchmarking Post-quantum Cryptography in TLS

for updates

Get Access

5

# 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  $\approx$  30% application slowdown
- 25% PQ TLS 1.3 handshake slowdown  $\approx$  25% slower browser experience



# What is perceived performance?

## Google PageSpeed Insights

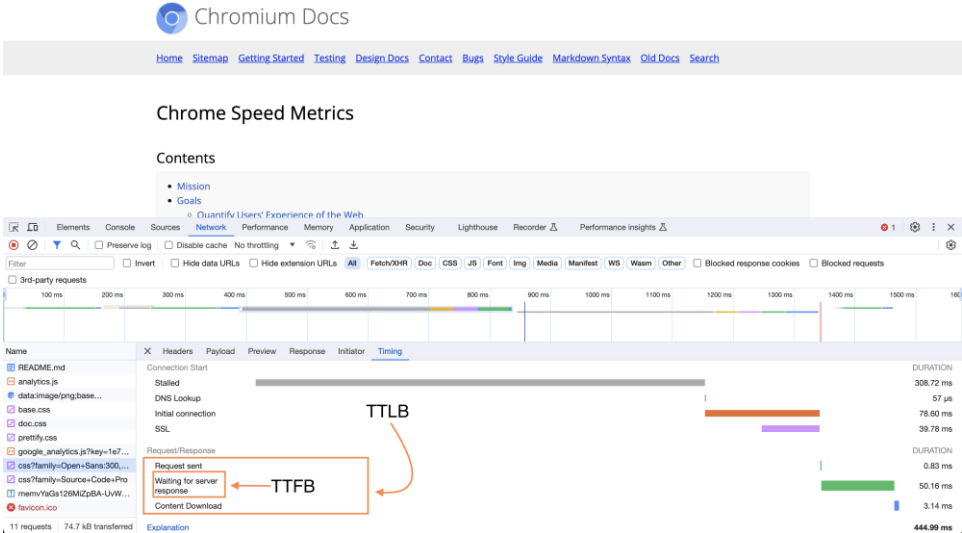
- First Contentful Paint (FCP)
- Largest Contentful Paint (LCP)
- (Experimental) Time to First Byte (TTFB)
- Cumulative Layout Shift (CLS)
- Interaction to Next Paint (INP)

Loading page content

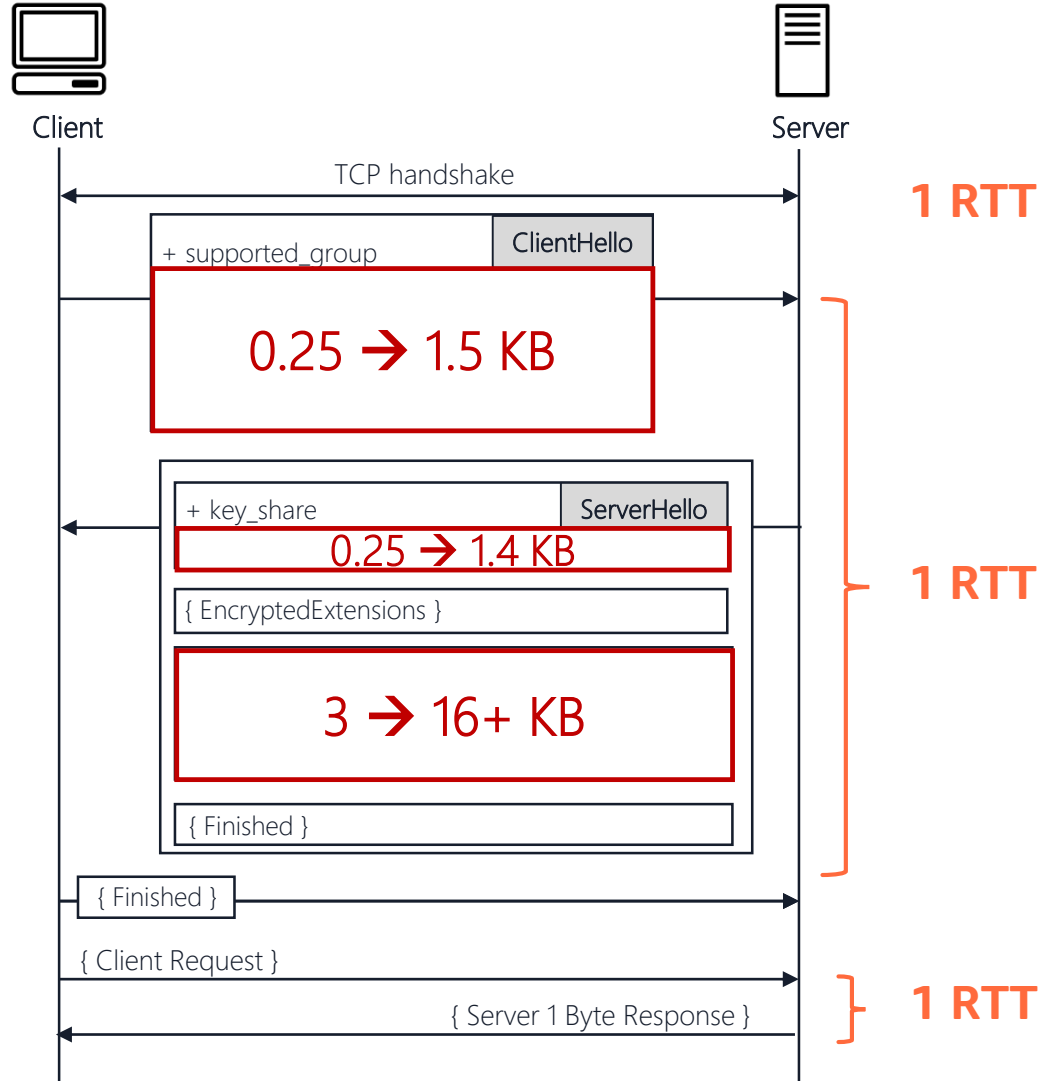
DNS redirect +  
TLS +  
Redirect time +  
request-response

After page is loaded

## Other Applications

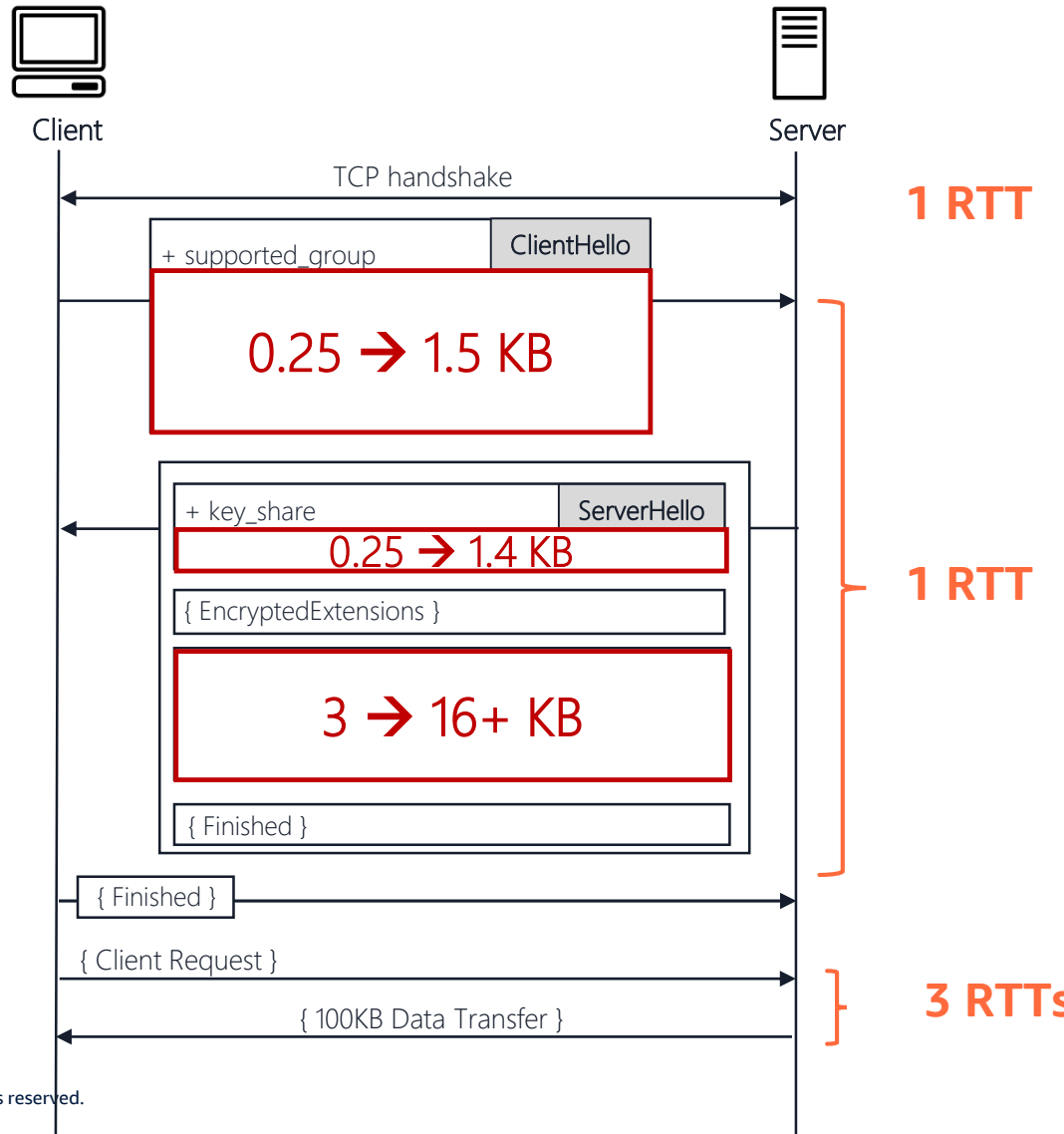


# Why? - TLS 1.3 handshake vs TTFB



If the PQ ephemeral public key and certs introduce an extra  $x$  ms, the handshake % increase is  $H=x/2RTT$ .  
The TTFB % increase is  $x/3RTT$   
( $=0.66*H$ ).

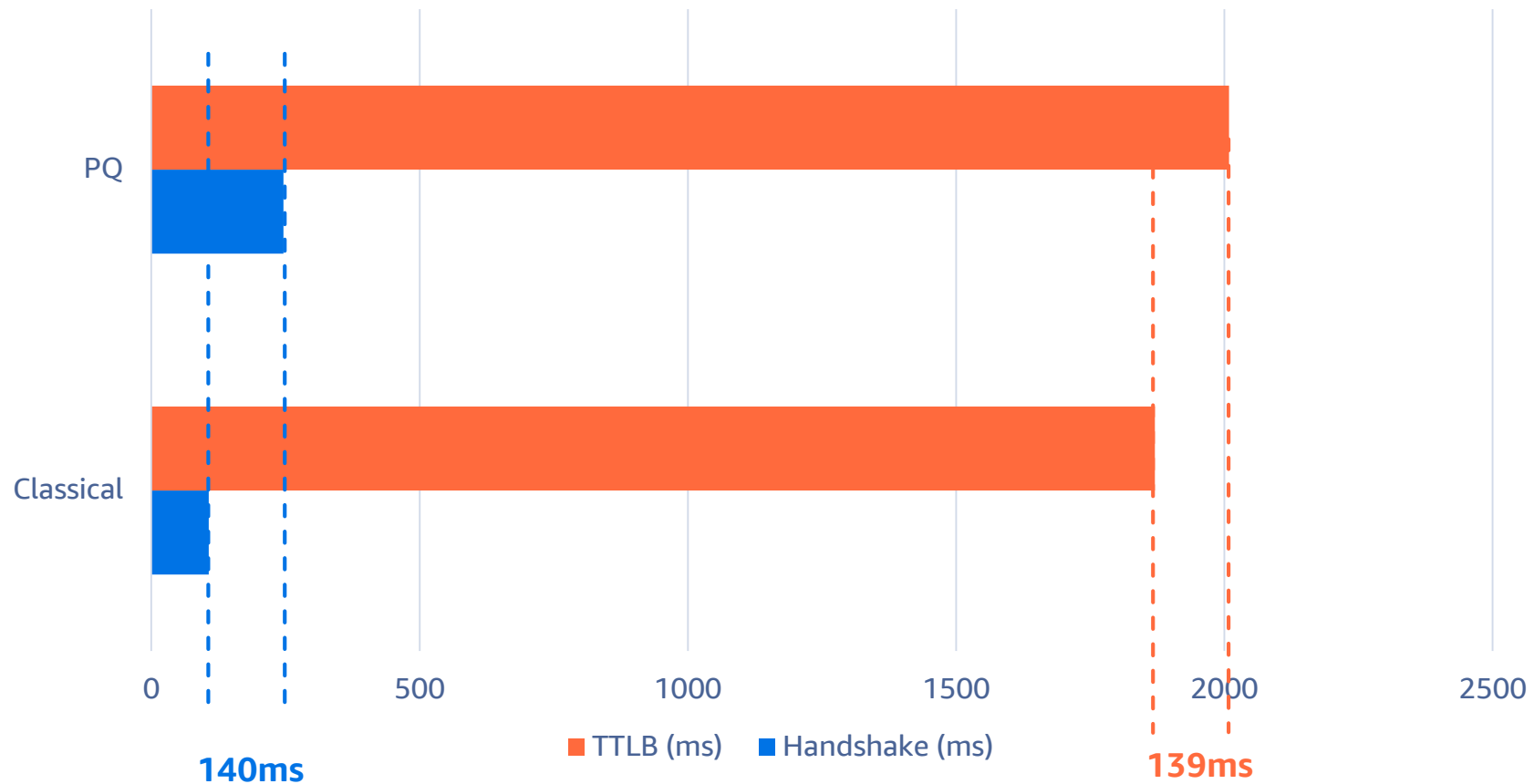
# Why? - TLS 1.3 handshake vs TTFB vs TTLB



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

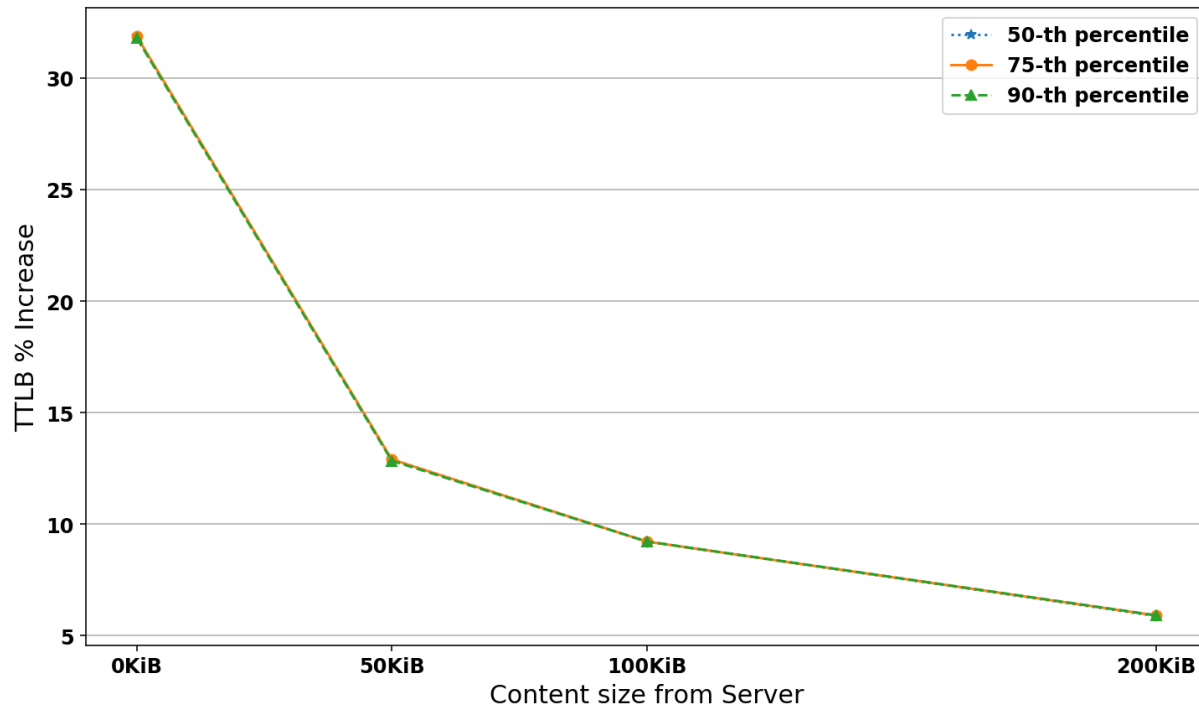




# TTLB % increase

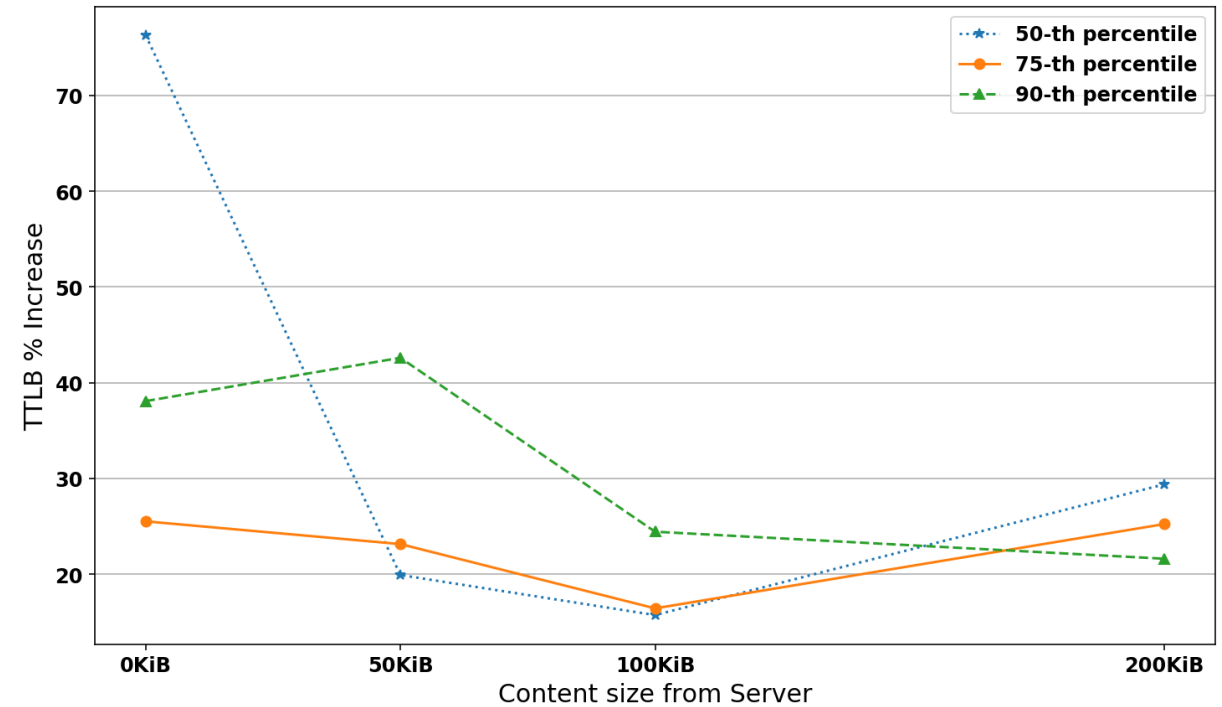
1MBPS, 200MS RTT, INITCWND=20MSS

## 0% loss



The classical connection TTLB percentiles at 200KiB are 2.3 seconds

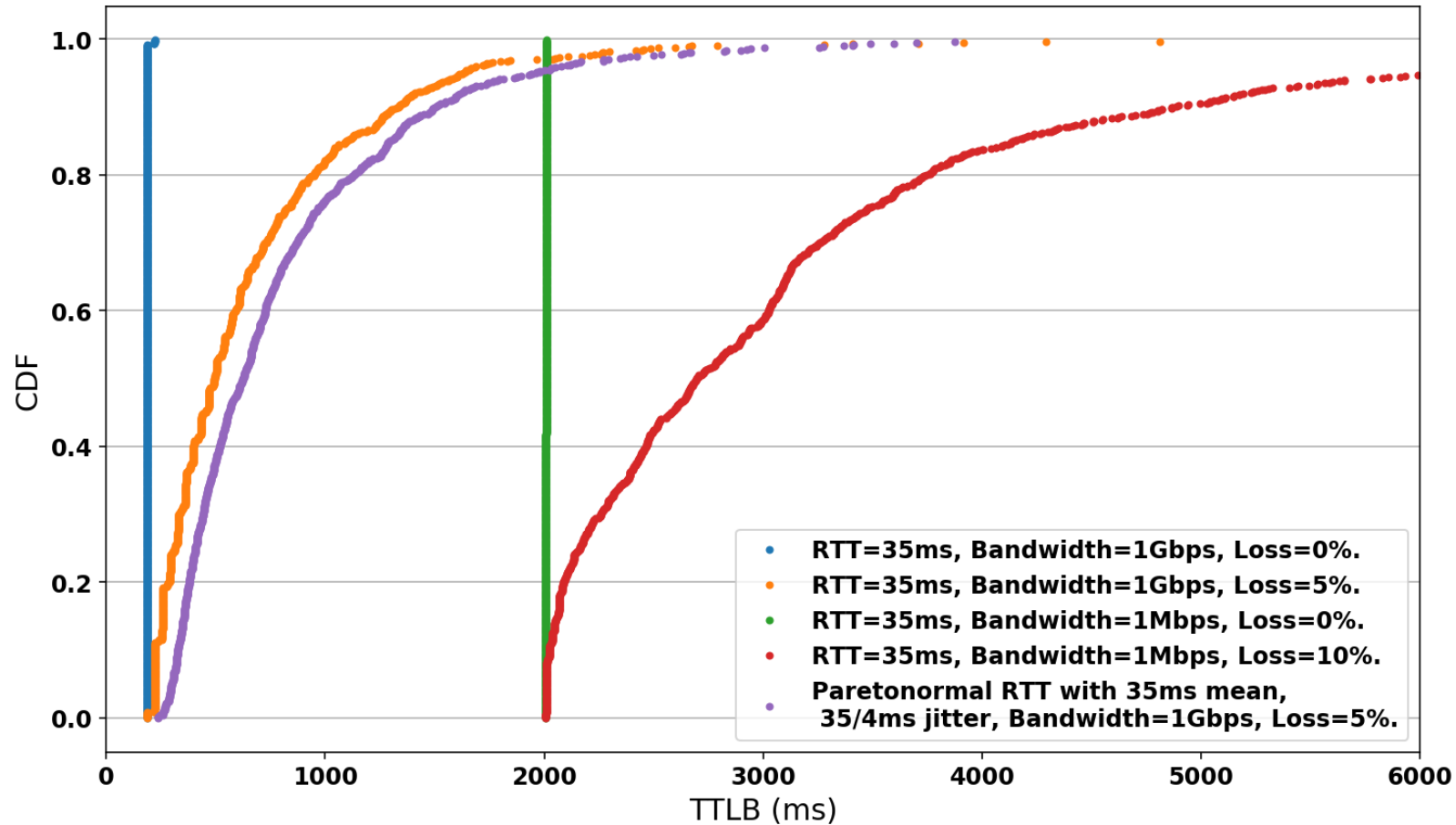
## 10% loss



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