ETSI/IQC Quantum Safe Cryptography Event

The effects of Dilithium on QUIC's performance

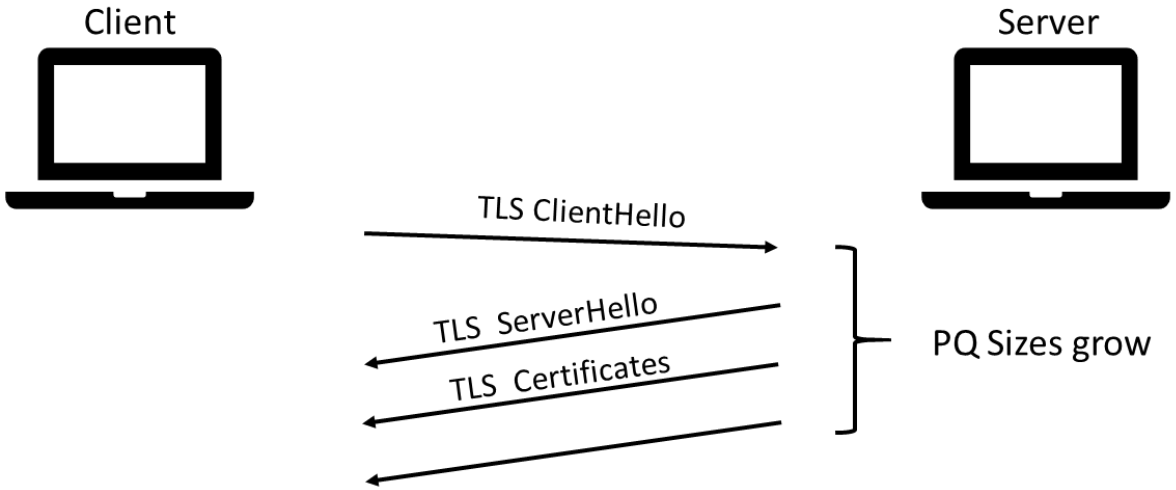
Panos Kampanakis

aws

02/14/2023

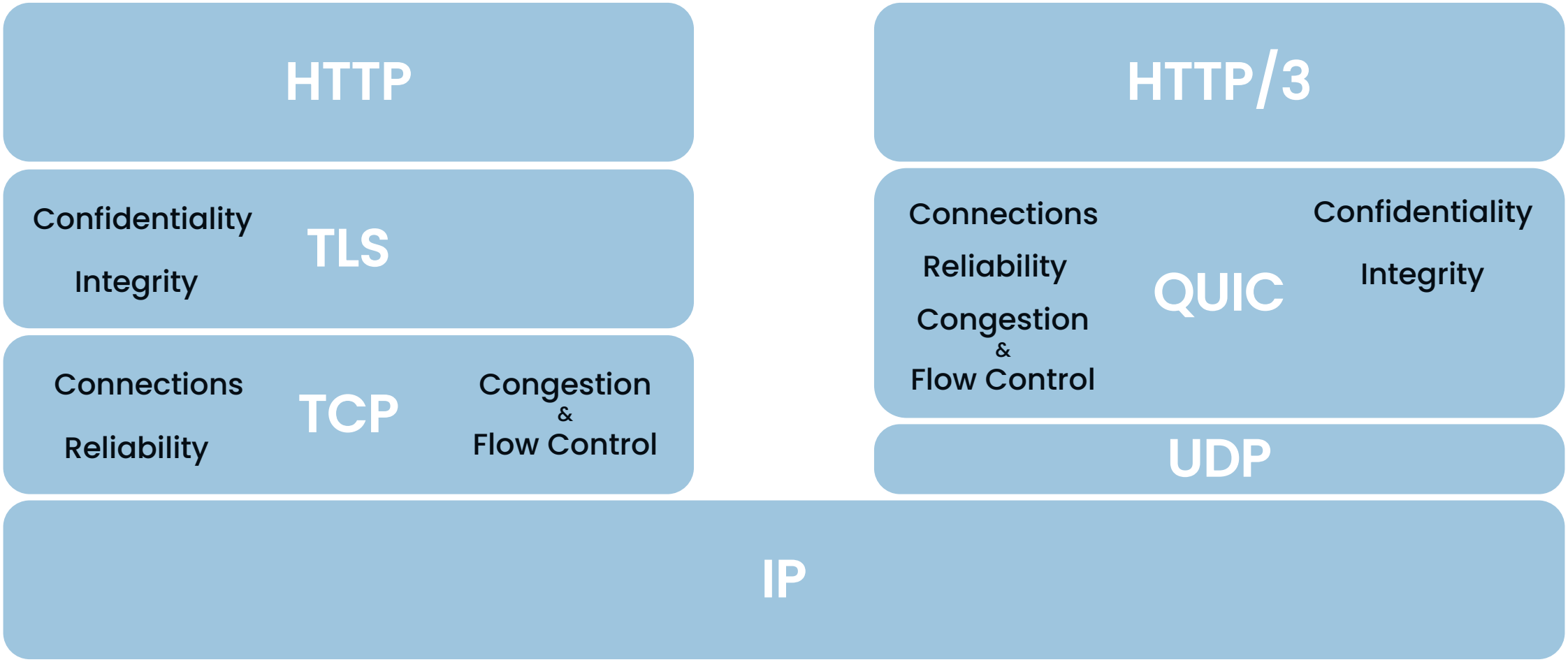
Background: Dilithium's Impact on TLS performance

- PQ key exchange will affect handshakes, but not detrimentally [CECPQ2] [iacr19-1447] [CON20]
- Authentication will have more impact [NDSS20] [CF21]
- Size of "authentication data" increases significantly [CSCML22]



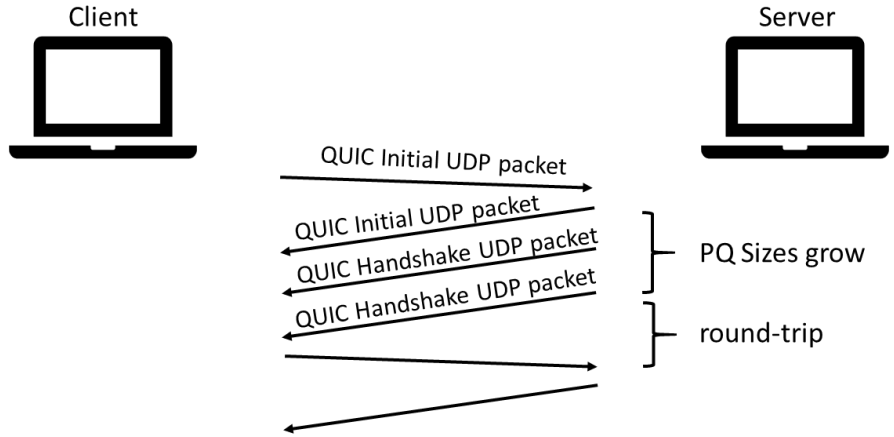
Takeaway: Slowdowns by Dilithium or any other PQ signature algorithm…

What is QUIC?

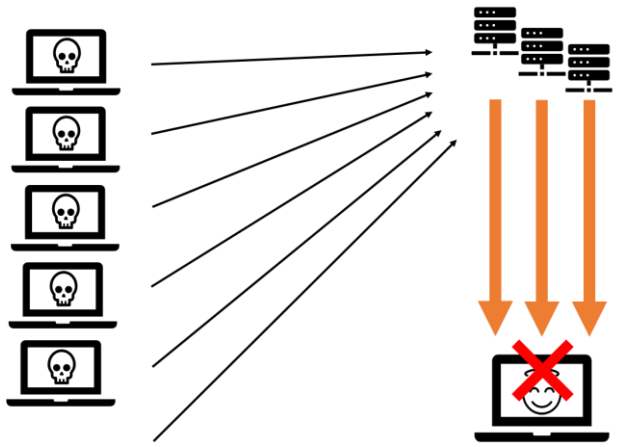

HTTP
Confidentiality
Integrity
TLS
Connections
Reliability
TCP
Congestion
&
Flow Control
IP
HTTP/3
Connections
Reliability
Congestion
&
Flow Control
QUIC
Confidentiality
Integrity
UDP

Intuitions about Dilithium's Impact on QUIC?

- QUIC's PQ
  - keys grow to 1-2KB (w. Kyber) and
  - "authentication data" to 17+ KB.



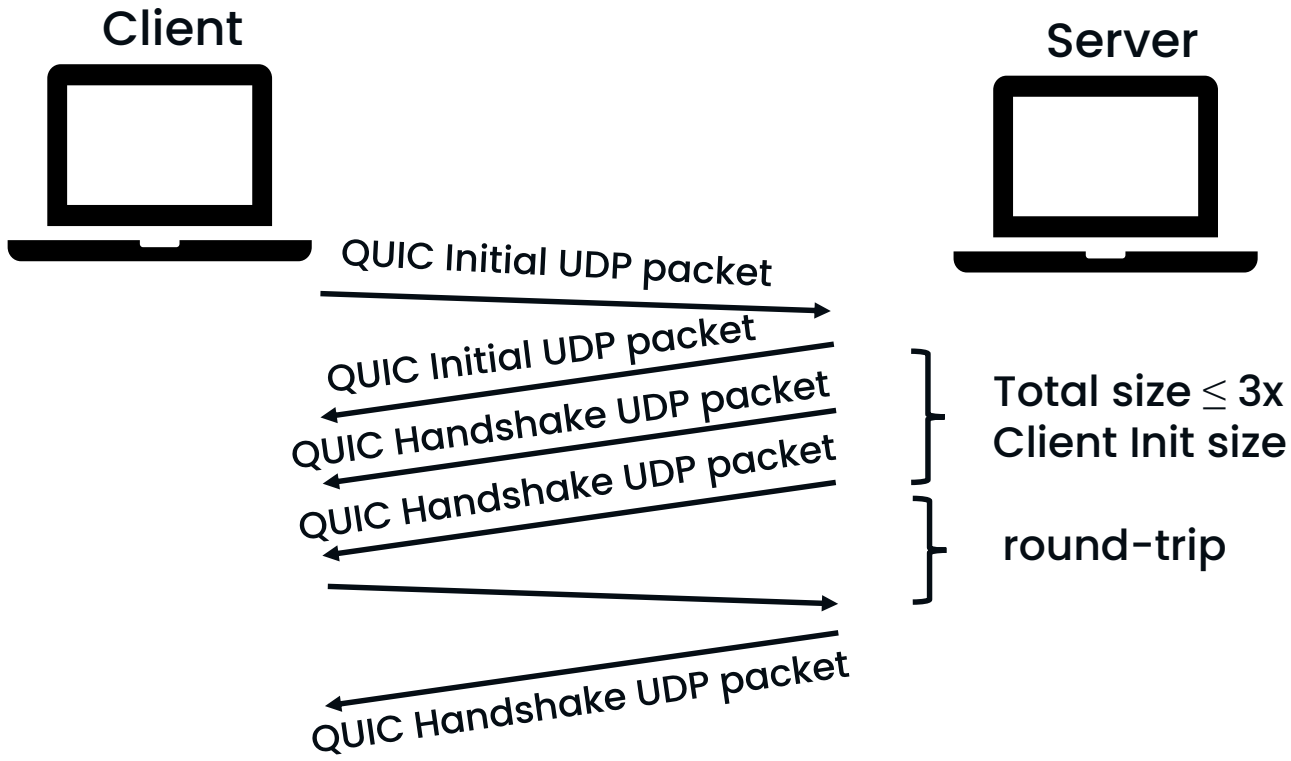
- Higher total loss probability [iacr19-1447]
- Extra Round-trip due to the ~4KB Amplification Window [CSCML22]
- Extra Round-trip due to the ~15KB Initial Congestion Window [CON20]
- Unacceptable performance at the "tails" for >10KB of "authentication data" [CF21]
- Amplification Reflection risk



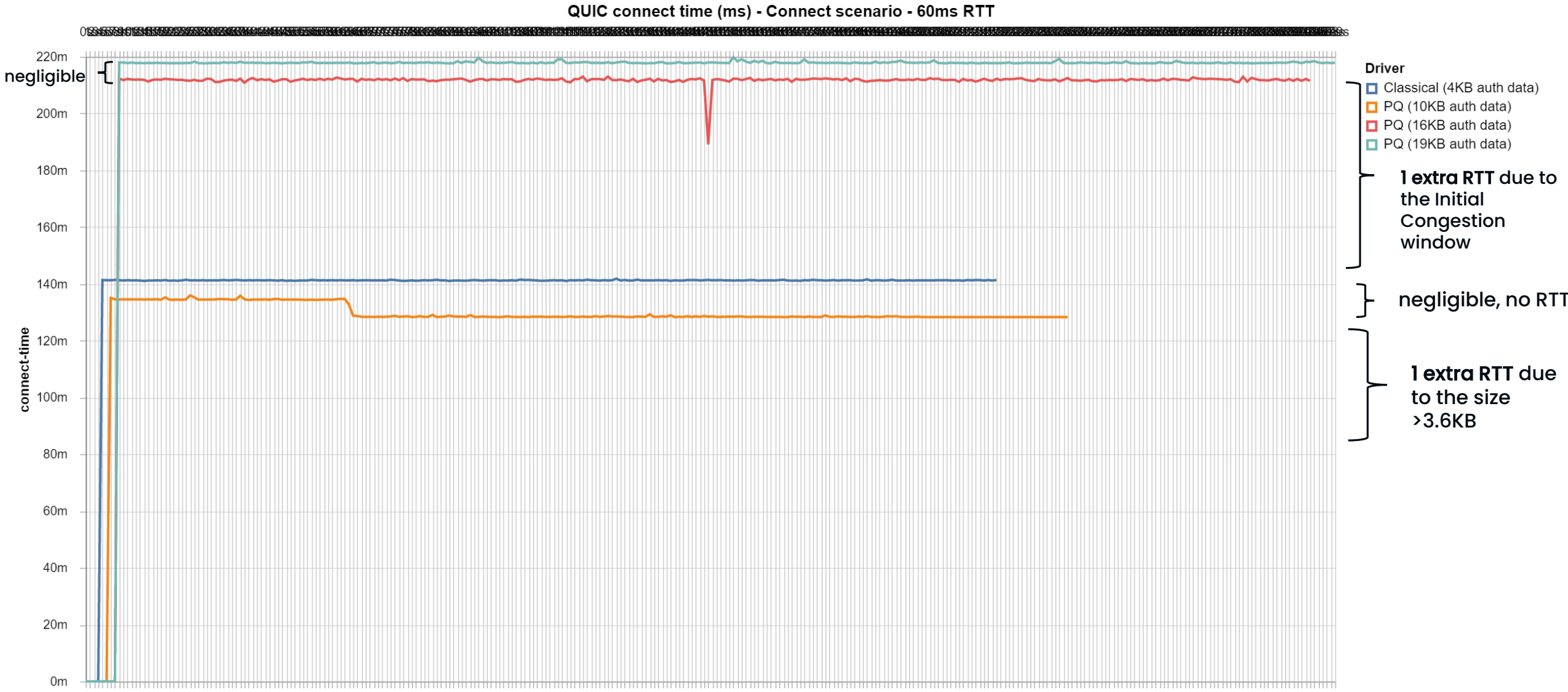
QUIC's Amplification Protection

- Even classical certificates can exceed the amplification window [CON22]
  - Some CDNs increase it to 6x or more.

- In a PQ world, we either accept an extra round-trip or increase the amplification factor by >4 [CSCML22].



Preliminary Experimental Results – QUIC connection time (60ms RTT)



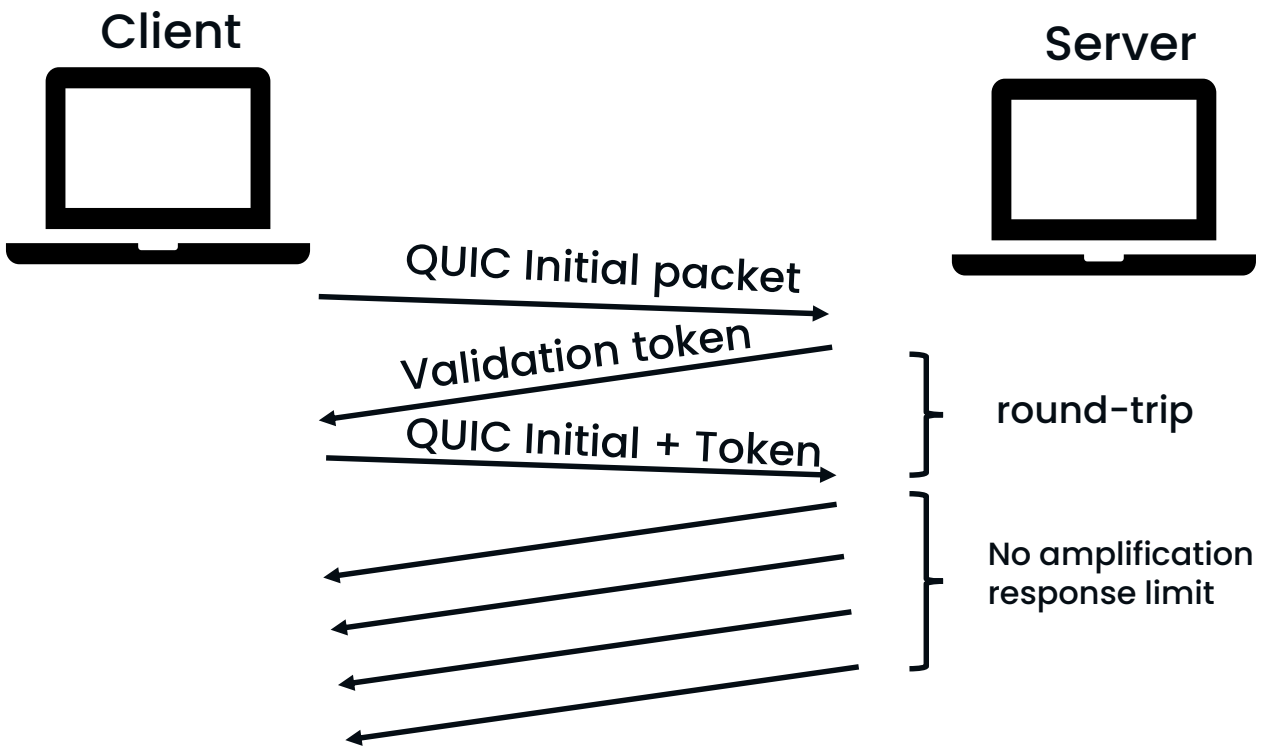
Solution Options

- ~~Artificially inflate the Client request~~
- Trim down “authentication data” by
  - caching CA certificates [CSCML22] [tls-scas] or
  - using session resumption
- Increase the Amplification Protection Window
  - at the cost of increasing the amplification factor
- Use Address validation tokens

About Address Validation Tokens

- Upon return with the server token, the client proves it is not spoofing.
- The first time, there is an extra round-trip.
- The round-trip is amortized if the client revisits the server with the same token.

- **Open question**: Would tokens speed up PQ connections?



Takeaways

QUIC will see performance slowdowns from Dilithium or other PQ signatures.

We need to research and decide what to do with QUIC's

- Size of the authentication data
- Amplification Protection
- Initial Congestion Window

Thank you!

kpanos@amazon.com