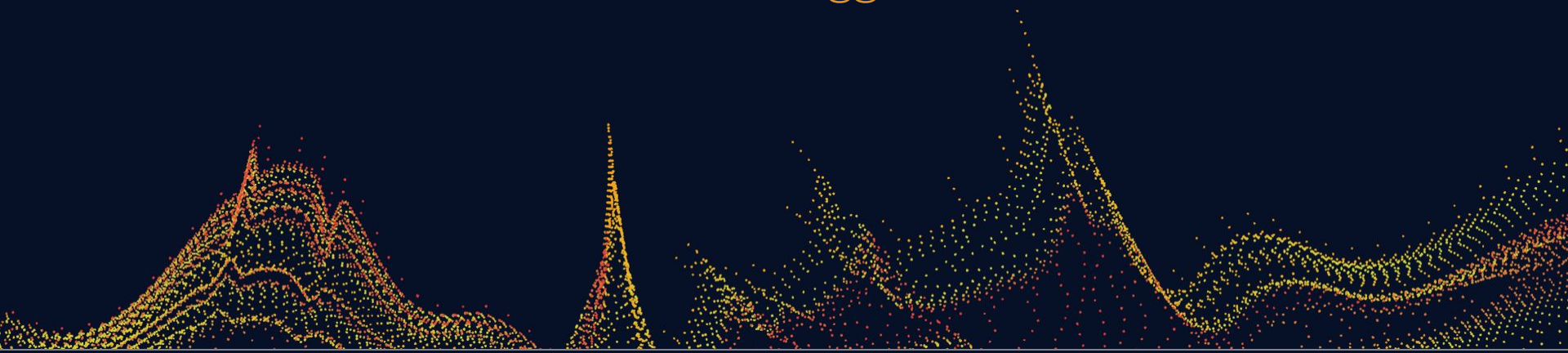
PQSHIELD

Weighing Post-Quantum Authentication

Thom Wiggers



The public key crypto in the TLS handshake

- ClientHello
  - 1 public key
- ServerHello
  - 1 ~~public key~~ ciphertext
- Server Certificates
  - Leaf certificate: 1 public key, 1 signature
  - Intermediate Certificate: 1 public key, 1 signature
  - Bonus content: 3x Certificate Transparency
- Server CertificateVerify
  - 1 signature

- Not pictured:
  - OCSP (Stapling)

The public key crypto in the TLS handshake

	Key Exchange	Handshake sig	Leaf pk	Leaf cert sig	Int CA pk	Int CA cert sig	Certificate Transparency	Total size	Root CA algorithm
Classic EC	X25519	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3 ECDSA P-256	**626**	ECDSA P-256
	64	72	65	72	65	72	216		
Current deployment	X25519MLKEM768	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3 ECDSA P-256	**2194**	ECDSA P-256
	1632	72	65	72	65	72	216		

The public key crypto in the TLS handshake

	Key Exchange	Handshake sig	Leaf pk	Leaf cert sig	Int CA pk	Int CA cert sig		Certificate Transparency	Total size	Root CA algorithm
Classic EC	X25519	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**626**	ECDSA P-256
	64	72	65	72	65	72		216		
Current deployment	X25519MLKEM768	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**2194**	ECDSA P-256
	1632	72	65	72	65	72		216		
ML-DSA Level II	X25519MLKEM768	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	3	ML-DSA-44	**18776**	ML-DSA-44
	1632	2420	1312	2420	1312	2420		7260		

The public key crypto in the TLS handshake

	Key Exchange	Handshake sig	Leaf pk	Leaf cert sig	Int CA pk	Int CA cert sig		Certificate Transparency	Total size	Root CA algorithm
Classic EC	X25519	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**626**	ECDSA P-256
	64	72	65	72	65	72		216		
Current deployment	X25519MLKEM768	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**2194**	ECDSA P-256
	1632	72	65	72	65	72		216		
ML-DSA Level II	X25519MLKEM768	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	3	ML-DSA-44	**18776**	ML-DSA-44
	1632	2420	1312	2420	1312	2420		7260		
ML-DSA Level V	SecP384r1MLKEM1024	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	3	ML-DSA-87	**36276**	ML-DSA-87
	3330	4627	2592	4627	2592	4627		13881		

The public key crypto in the TLS handshake

	Key Exchange	Handshake sig	Leaf pk	Leaf cert sig	Int CA pk	Int CA cert sig		Certificate Transparency	Total size	Root CA algorithm
Classic EC	X25519	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**626**	ECDSA P-256
	64	72	65	72	65	72		216		
Current deployment	X25519MLKEM768	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**2194**	ECDSA P-256
	1632	72	65	72	65	72		216		
ML-DSA Level II	X25519MLKEM768	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	3	ML-DSA-44	**18776**	ML-DSA-44
	1632	2420	1312	2420	1312	2420		7260		
ML-DSA Level V	SecP384r1MLKEM1024	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	3	ML-DSA-87	**36276**	ML-DSA-87
	3330	4627	2592	4627	2592	4627		13881		
Falcon	X25519MLKEM768	Falcon-512	Falcon-512	Falcon-512	Falcon-512	Falcon-512	3	Falcon-512	**7422**	Falcon-512
	1632	666	897	666	897	666		1998		

* Falcon is difficult to implement correctly!

The public key crypto in the TLS handshake

	Key Exchange	Handshake sig	Leaf pk	Leaf cert sig	Int CA pk	Int CA cert sig		Certificate Transparency	Total size	Root CA algorithm
Classic EC	X25519	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**626**	ECDSA P-256
	64	72	65	72	65	72		216		
Current deployment	X25519MLKEM768	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**2194**	ECDSA P-256
	1632	72	65	72	65	72		216		
ML-DSA Level II	X25519MLKEM768	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	3	ML-DSA-44	**18776**	ML-DSA-44
	1632	2420	1312	2420	1312	2420		7260		
ML-DSA Level V	SecP384r1MLKEM1024	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	3	ML-DSA-87	**36276**	ML-DSA-87
	3330	4627	2592	4627	2592	4627		13881		
Falcon	X25519MLKEM768	Falcon-512	Falcon-512	Falcon-512	Falcon-512	Falcon-512	3	Falcon-512	**7422**	Falcon-512
	1632	666	897	666	897	666		1998		
Falcon level V	SecP384r1MLKEM1024	Falcon-1024	Falcon-1024	Falcon-1024	Falcon-1024	Falcon-1024	3	Falcon-1024	**14596**	Falcon-1024
	3330	1280	1793	1280	1793	1280		3840		

The public key crypto in the TLS handshake

	Key Exchange	Handshake sig	Leaf pk	Leaf cert sig	Int CA pk	Int CA cert sig		Certificate Transparency	Total size	Root CA algorithm
Classic EC	X25519	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**626**	ECDSA P-256
	64	72	65	72	65	72		216		
Current deployment	X25519MLKEM768	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**2194**	ECDSA P-256
	1632	72	65	72	65	72		216		
ML-DSA Level II	X25519MLKEM768	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	3	ML-DSA-44	**18776**	ML-DSA-44
	1632	2420	1312	2420	1312	2420		7260		
ML-DSA Level V	SecP384r1MLKEM1024	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	3	ML-DSA-87	**36276**	ML-DSA-87
	3330	4627	2592	4627	2592	4627		13881		
Falcon	X25519MLKEM768	Falcon-512	Falcon-512	Falcon-512	Falcon-512	Falcon-512	3	Falcon-512	**7422**	Falcon-512
	1632	666	897	666	897	666		1998		
Falcon level V	SecP384r1MLKEM1024	Falcon-1024	Falcon-1024	Falcon-1024	Falcon-1024	Falcon-1024	3	Falcon-1024	**14596**	Falcon-1024
	3330	1280	1793	1280	1793	1280		3840		
Optimized	X25519MLKEM768	ML-DSA-44	ML-DSA-44	Falcon-512	Falcon-512	Falcon-512	3	Falcon-512	**9591**	Falcon-512
	1632	2420	1312	666	897	666		1998		

The public key crypto in the TLS handshake

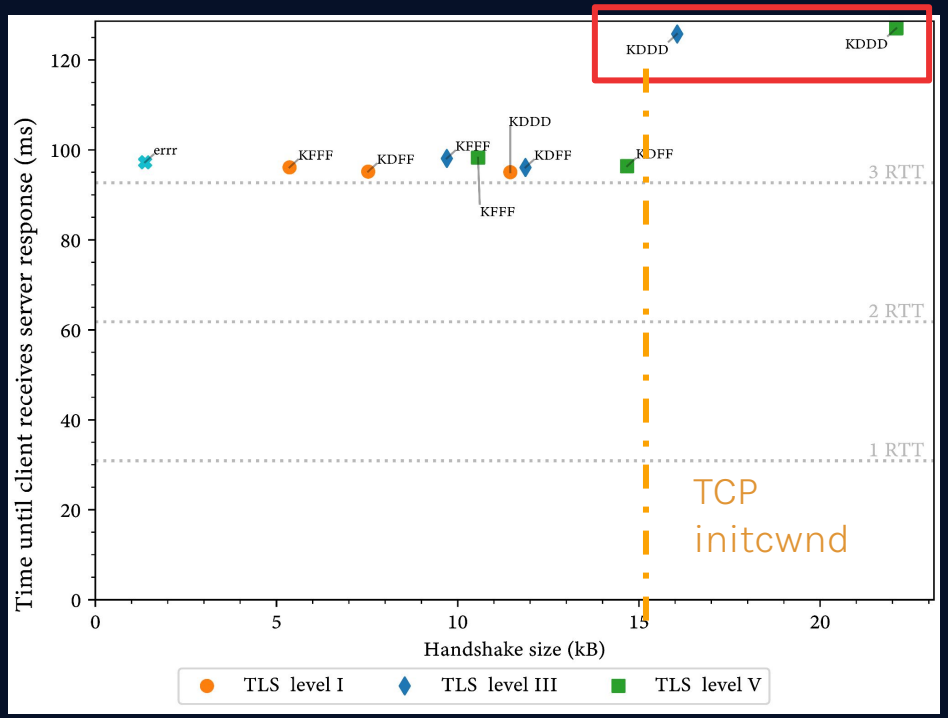
	Key Exchange	Handshake sig	Leaf pk	Leaf cert sig	Int CA pk	Int CA cert sig		Certificate Transparency	Total size	Root CA algorithm
Classic EC	X25519	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**626**	ECDSA P-256
	64	72	65	72	65	72		216		
Current deployment	X25519MLKEM768	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**2194**	ECDSA P-256
	1632	72	65	72	65	72		216		
ML-DSA Level II	X25519MLKEM768	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	3	ML-DSA-44	**18776**	ML-DSA-44
	1632	2420	1312	2420	1312	2420		7260		
ML-DSA Level V	SecP384r1MLKEM1024	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	3	ML-DSA-87	**36276**	ML-DSA-87
	3330	4627	2592	4627	2592	4627		13881		
Falcon	X25519MLKEM768	Falcon-512	Falcon-512	Falcon-512	Falcon-512	Falcon-512	3	Falcon-512	**7422**	Falcon-512
	1632	666	897	666	897	666		1998		
Falcon level V	SecP384r1MLKEM1024	Falcon-1024	Falcon-1024	Falcon-1024	Falcon-1024	Falcon-1024	3	Falcon-1024	**14596**	Falcon-1024
	3330	1280	1793	1280	1793	1280		3840		
Optimized	X25519MLKEM768	ML-DSA-44	ML-DSA-44	Falcon-512	Falcon-512	Falcon-512	3	Falcon-512	**9591**	Falcon-512
	1632	2420	1312	666	897	666		1998		
Optimized MAYO	X25519MLKEM768	MAYO-1	MAYO-1	MAYO-1	MAYO-1	MAYO-2	3	MAYO-2	**6124**	MAYO-2
	1632	454	1420	454	1420	186		558		

Preface

- All lattice-based PQC algorithms are **stupid fast** on smartphones, computers
- All effects in benchmarks can be attributed to **sizes**

Synthetic Benches

- 1000mbps, 31ms RTT latency
- First RTT: TCP SYN/ACK
- Second RTT: TLS Handshake
- Third RTT: tiny HTTP Request / Response



Label XABC:
X: Key exchange
A: Handshake auth
B: Intermediate Certificate
C: Root CA certificate

errr: X25519+RSA2048
K: Kyber
D: Dilithium
F: Falcon

No SCTs!

Source: "Post-Quantum TLS", Thom Wiggers, PhD thesis. 2024

The public key crypto in the TLS handshake

	Key Exchange	Handshake sig	Leaf pk	Leaf cert sig	Int CA pk	Int CA cert sig		Certificate Transparency	Total size	Root CA algorithm
Classic EC	X25519	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**626**	ECDSA P-256
	64	72	65	72	65	72		216		
Current deployment	X25519MLKEM768	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256	3	ECDSA P-256	**2194**	ECDSA P-256
	1632	72	65	72	65	72		216		
ML-DSA Level II	X25519MLKEM768	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	ML-DSA-44	3	ML-DSA-44	**18776**	ML-DSA-44
	1632	2420	1312	2420	1312	2420		7260		
ML-DSA Level V	SecP384r1MLKEM1024	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	ML-DSA-87	3	ML-DSA-87	**36276**	ML-DSA-87
	3330	4627	2592	4627	2592	4627		13881		
Falcon	X25519MLKEM768	Falcon-512	Falcon-512	Falcon-512	Falcon-512	Falcon-512	3	Falcon-512	**7422**	Falcon-512
	1632	666	897	666	897	666		1998		
Falcon level V	SecP384r1MLKEM1024	Falcon-1024	Falcon-1024	Falcon-1024	Falcon-1024	Falcon-1024	3	Falcon-1024	**14596**	Falcon-1024
	3330	1280	1793	1280	1793	1280		3840		
Optimized	X25519MLKEM768	ML-DSA-44	ML-DSA-44	Falcon-512	Falcon-512	Falcon-512	3	Falcon-512	**9591**	Falcon-512
	1632	2420	1312	666	897	666		1998		
MAYO	X25519MLKEM768	MAYO-1	MAYO-1	MAYO-1	MAYO-1	MAYO-2	3	MAYO-2	**6124**	MAYO-2
	1632	454	1420	454	1420	186		558		

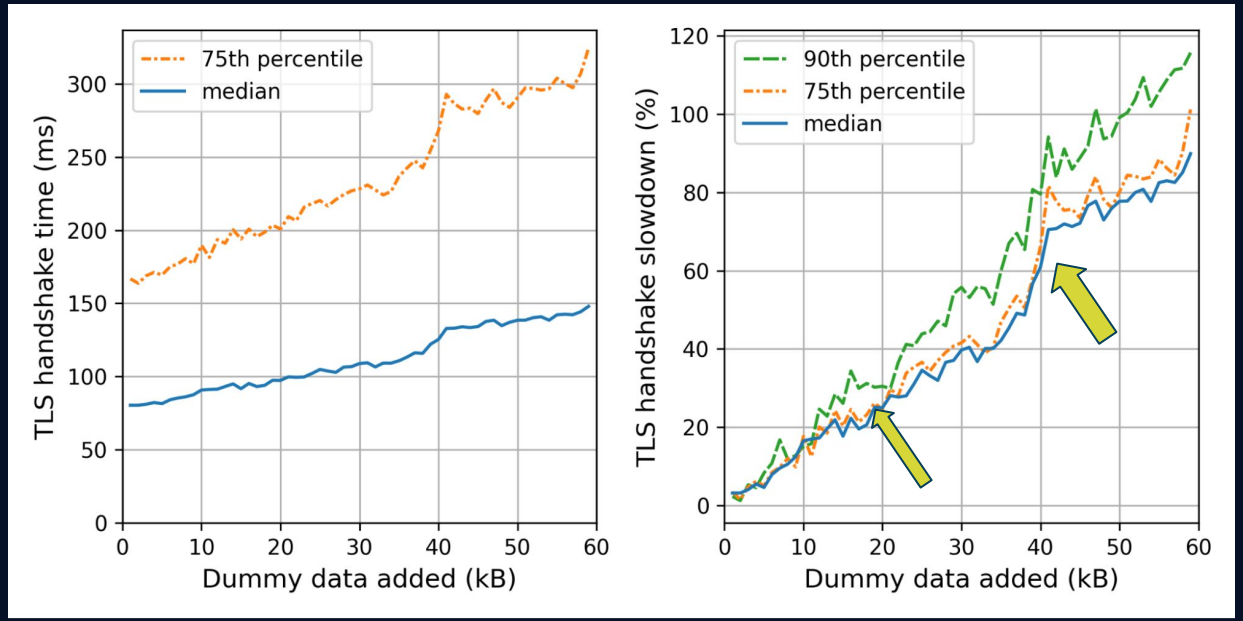
Practical benchmarks

Slowdown more gradual than synthetic benchmark

25% slowdown predicted for ML-DSA-44 (~18k).

Note: Cloudflare has initcwnd of 30 MSS, “cliff” may need to be moved to the left!

(someone please inform the protocol police of this violation of RFC 6928)



Src: Sizing Up Post-Quantum Signatures by Bas Westerbaan

Some random server operator

“So I need to add 15kB to the handshake, potentially slowing down my website by 20%, for something that doesn’t exist today?”

But we do want this guy to deploy PQC!

Google Chrome's take

"Transmitting Kyber keys is quite slow. The extra size from Kyber causes the TLS ClientHello to be split into two packets, resulting in a 4% median latency increase to all TLS handshakes in Chrome on desktop."

Chromium Blog: Advancing Our Amazing Bet on Asymmetric Cryptography

"Adding ~7KB is implausible unless a cryptographically relevant quantum computer (CRQC) is tangibly imminent."

Google Chrome Security Building a Deployable Post-quantum Web PKI

Are things this dire?

- Panos Kampanakis & Will Childs-Klein. The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections
  - "The time-to-**last**-byte increase stays below 5% for high-bandwidth, stable networks. It goes from 32% increase of the handshake time to under 15% increase of the time-to-last-byte when transferring 50KiB of data or more under low-bandwidth, stable network conditions.

- Cloudflare: "The median number of bytes transferred from server-to-client over a resumed QUIC connection is 4.4kB, while the average is 395kB. For non-resumptions the median is 7.8kB and average is 551kB.