Two PQ Signature Use-cases

Non-issues, challenges and potential solutions.

Panos Kampanakis – Dimitrios Sikeridis
Cisco Systems – Univ. of New Mexico
09/07/2019

This work

Evaluation of PQ signatures for

- Image signing
- TLS 1.3

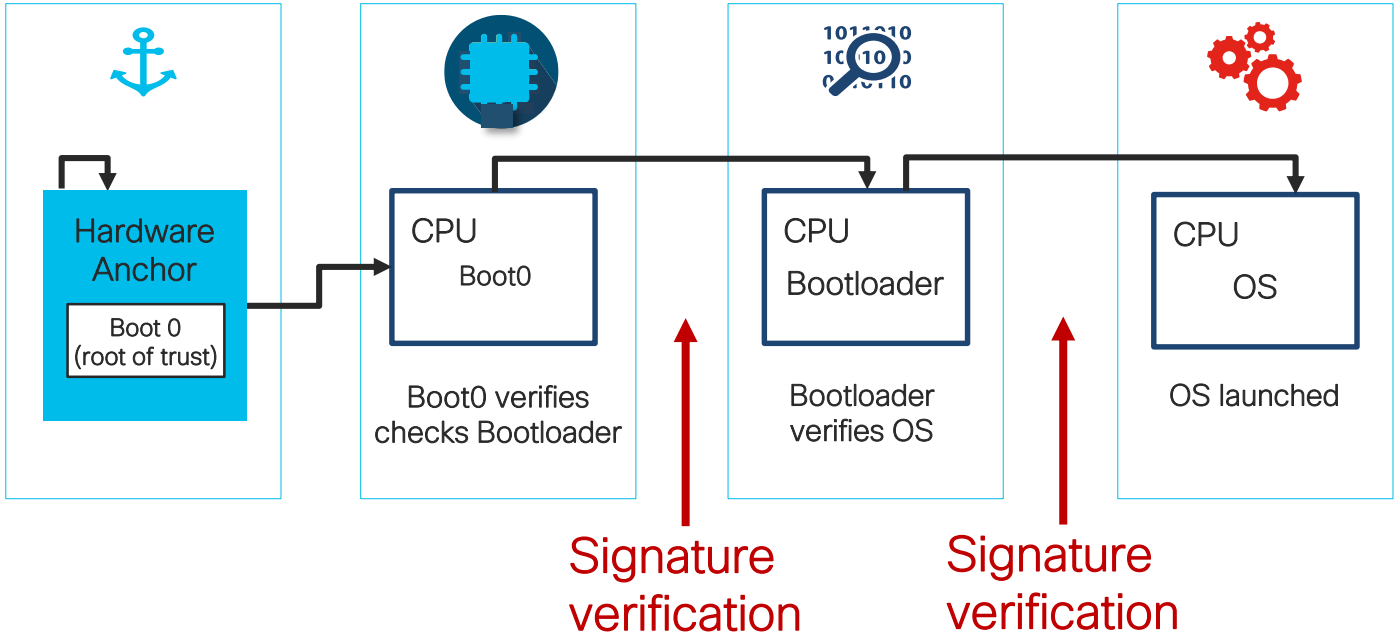
Uploaded in eprint.

Why is Cisco interested?

- We sign our software and boot images
- Encryption and Authentication is used in products
  - TLS / WebVPN
  - IKEv2 / IPSec VPNs
  - Encrypted Voice
- Encourage adoption of next generation crypto

PQ Signatures in Secure Boot

Secure Boot



(Some of our) Experimental Findings

Parameter	PK (B)	Sig (KB)	Verifier code (KB)	Sign (ms)	Verify (ms)
LMS_SHA256_M32_H15 with LMOTS_SHA256_N32_W8	60	1.63	2.15	6.24	1.30
LMS_SHA256_M32_H20 with LMOTS_SHA256_N32_W4	60	2.83	2.57	1.46	0.17
HSS $L = 3$ with LMS256H15W4, LMS256H10W4, LMS256H10W4	60	7.80	3.15	1.71	0.48
SPHINCS$^+$ $n = 24$, $H = 15$, $d = 3$, $k = 18$, $a = 13$ $w = 256$	48	8.30	4.41	150.9	3.20
SPHINCS$^+$ $n = 24$, $H = 20$, $d = 4$, $k = 18$, $a = 13$ $w = 16$	48	11.49	4.46	83.4	0.63
SPHINCS$^+$ $n = 24$, $H = 35$, $d = 5$, $k = 20$, $a = 12$ $w = 16$	48	13.22	4.50	96.6	0.72
SPHINCS$^+$ $n = 32$, $H = 15$, $d = 3$, $k = 19$, $a = 16$ $w = 256$	64	14.11	4.47	677.8	4.19
SPHINCS$^+$ $n = 32$, $H = 20$, $d = 4$, $k = 19$, $a = 16$ $w = 16$	64	19.58	4.54	595.6	0.80
SPHINCS$^+$ $n = 32$, $H = 35$, $d = 5$, $k = 21$, $a = 15$ $w = 16$	64	22.62	4.53	370.2	0.95

Signing < 0.5s

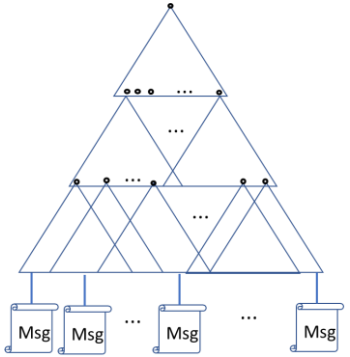
Verification <5ms

Miniscule PKs.

Signatures 1.5–22.5KB

Verifier code <5KB

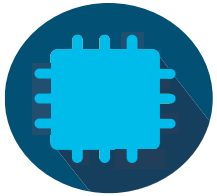
PQ image signing: Non-Issues



- HBS signatures
  - Non-issue for most usecases.
  - Two or three level tree hierarchy.
- Revocation can be done in a straightforward manner.
- More constrained use-cases
  - could use Stateful HBS.
    - CAREFUL with the state!

PQ image signing: Challenges

- For complete secure boot,
  - we need more chip vendors to buy in.

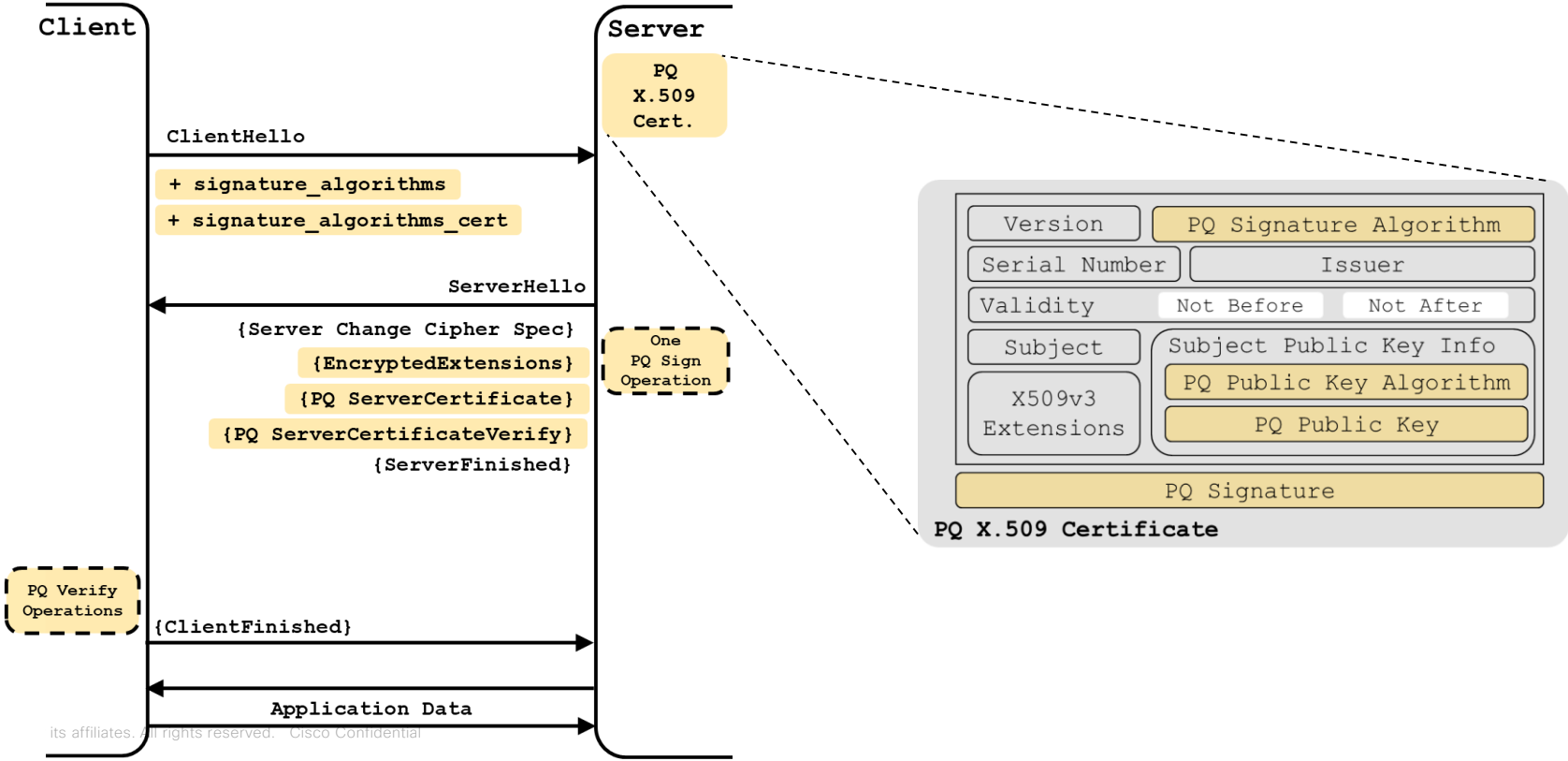


- NIST approval of SPHINCS+ is still to be seen.
- NIST approval of Stateful HBS for FIPS?
  - Will state management be FIPS certified?

NIST

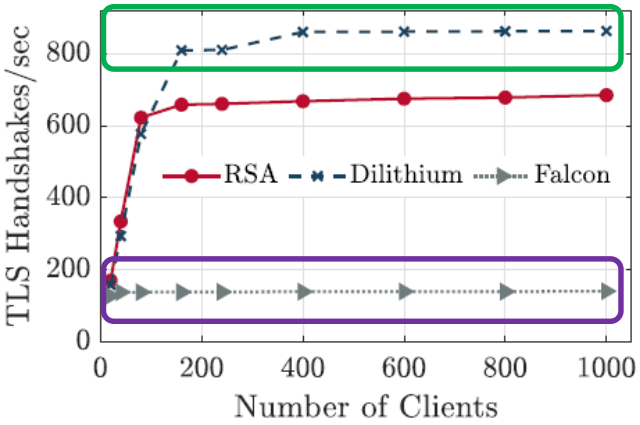
PQ Signatures in TLS 1.3

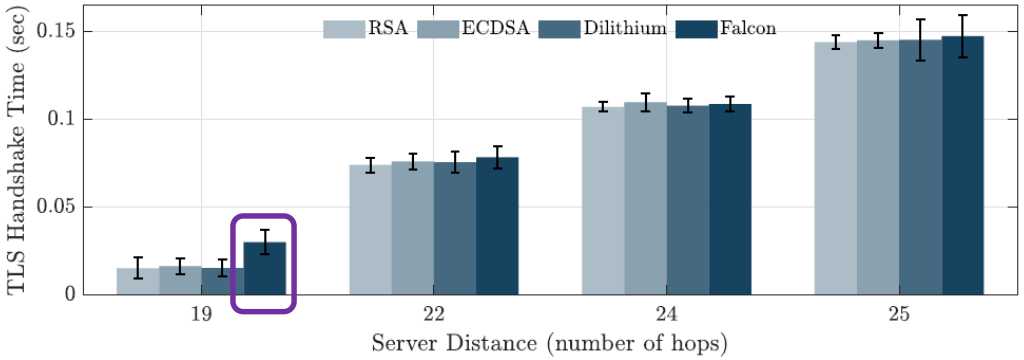
TLS 1.3 Handshake and PQ X.509 Certificate



(Some of our) Experimental Findings

Signature Algorithm	Latency (%) 50^{th}	95^{th}
Falcon	7.9	3.9
Dilithium	6.3	2.8
Hash-based (SPHINCS+)	321.1	296.9





PQ authenticated tunnels: Non-Issues

- VPNs (DTLS, IKEv2) would not suffer by slower PQ Authentication
  - Tunnel establishment takes ~5 seconds
  - Tunnels are long-lived.
  - Authentication does not take place often.
  - Signing and verification are more important for a heavily loaded head-ends.

PQ authenticated tunnels: Challenges

- Web connections will be more impacted
  - Short-lived
  - Relatively small amounts of data per connection.
  - How much slowdown will end up annoying a user?...
- Dilithium and Falcon
  - Level 1 perform OK but do not have sufficient classical security
  - Level 3,5 double the TLS 1.3 handshake time
  - Dilithium Level 2 performs better than Level 3, close to Level 1.

PQ authenticated tunnels: Challenges (cont'd)

- If Dilithium and Falcon are not standardized
  - (D)TLS and PKI would need updates
    - ICA cert caching, offline cert downloads, KEM based authentication.
- ICA cert caching and suppression [draft-thomson-tls-sic] would significantly improve performance.

Summary

- HBS can be used for
  - image signing for most use-cases.
- PQ most algorithms do
  - NOT heavily impact long-lived tunnels (e.g., VPNs, SSH)
  - Impact (D)TLS web applications but there are acceptable options and alleviation mechanisms.

IBM's Quantum Computer

Thank you!

Questions?

panosk@cisco.com