Why have the PQC standards taken so long?

Bottlenecks, bickering, and building momentum

Mike Ounsworth
OpenSSL Conf 2026

Since 2017 …

… we have known the general shape of Post Quantum Cryptography:

- Signatures behave the same as signatures today.
- KEMs behave differently from RSA Key Transport or ECDH Key Agreement.
- Public Keys, Signatures, Ciphertexts: ~ 5 kb.
- Performance: roughly the same as today.

NIST PQC Round 1 submissions closed Nov 30, 2017

Since 2023 and 2024 …

August 2023: The Initial Public Drafts (ipd) versions of FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) published.

- Allowed standards bodies and hardware / software vendors to begin designing for the specifics of these algorithms.

August 2024: Final versions of FIPS 203, 204, 205 published.

- Only minor changes from ipd versions.

Today, at the end of 2026 …

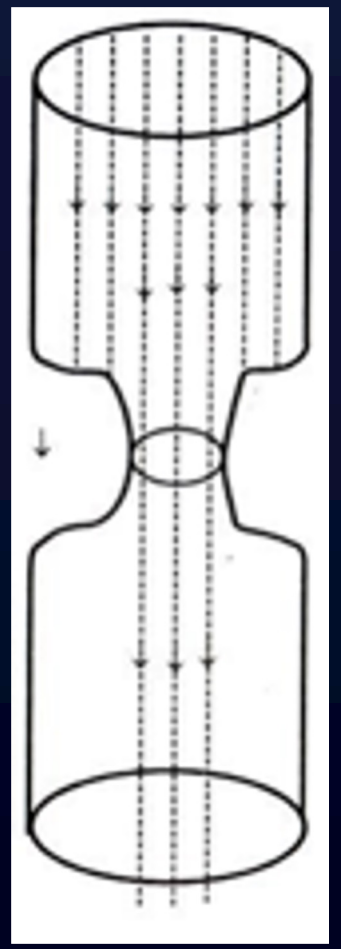
- We see PQC in the TLS key exchange (X25519MLKEM768).
- Very little else has started using PQC in production.
- In fact, we still don’t even have complete Internet Standards for PQC in many places:
  - ML-DSA or MTC Root CAs for TLS.
  - PQC in JWT
  - Hybrids / Composites
  - etc
- So, of course, we also don’t have hardware and software products.

Why??

Bottlenecks,

noun

1. The narrow part of a bottle near the top.
2. A narrow or obstructed section, as of a highway or a pipeline.
3. A point or an area of traffic congestion. A hindrance to progress or production.



Bickering,

noun

1. Petty quarreling. Usually considered a childish behaviour, although often applied to adults.
2. A quarrel about petty points.

See also: Bike-Shedding:

1. Debating the colour of paint on the employee bike shed instead of more important business topics.
2. Focusing on trivial and unimportant details.

Building Momentum,

Consensus

noun

1. An opinion or position reached by a group as a whole.
2. General agreement or accord.

Speaker Bio: Mike Ounsworth

```
Terminal
~

→  ~ cat whois_mike_ounsworth.txt
Mike Ounsworth wears many hats:

Lead maintainer of Bouncy Castle Rust crypto library
Adjunct Professor, Université de Sherbrooke, Canada

IETF:
  * Author of 4 RFCs and 12 active Internet Drafts
  * Chair of the ACME Working Group
  * Member of the Security Directorate review team



Past:
  * Software Security Architect and Appsec Tester, Entrust
  * #14 all-time ranked user on security.stackexchange.com
  * M.Sc Robotics, AI, McGill, Canada
  * B.Sc, CompSci, Math, Phys, Queen's University, Canada
→  ~
```

Bottlenecks

Engineering problems that needed solving

Bottlenecks:
Engineering problems that needed solving

- KEMs do not behave the same way as RSA Key Transport ECDH Key Agreement
  - KEMs cannot do a Proof-of-Possession, which is needed for CSRs. Needed redesign of:
    - CMPv3 ✅
    - CMC ✅
    - ACME (ongoing)
  - KEMs cannot do a Non-Interactive Key Exchange (NIKE), or a Non-Interactive Authenticated Key Exchange (NIAuthKEM).

In most cases, this meant adding an extra round-trip to the protocol.

Bottlenecks:

Engineering problems that needed solving

- Private keys
  - Lattice schemes allow two private key formats: seeds and “semi-expanded”.
  - Now all protocols like p11, p12, ssh, jwk, etc, need to decide to support Seeds, Keys, or Both.

- Pre-hashing
  - RSA and ECDSA did pre-hashing of the to-be-signed data as a separate pre-step. PQC signatures do not.
  - But some use cases require pre-hashing for privacy or performance reasons.
  - So we needed to design external pre-hashing back in.

Bottlenecks:
Engineering problems that needed solving

- Hybrid / Composite
  - Leaving aside the bickering (more on that later), how do you combine two signatures or two KEMs, and what security properties does that have?
  - Many years of design effort was spent trying to understand this:
    - LAMPS Composite Signatures and KEMs: 2019 - 2026
    - PQUIP RFC 9955 Hydrid Signature Spectrums: 2023 - 2026
    - X-Wing: 2024
    - CFRG Hybrid KEMs Design Team: 2024
    - draft-prabel-cfrg-suf-hybrid-sigs: 2025 - 2026

- Is this allowed under FIPS, or do the FIPS docs need to change?
  - NIST PQC FAQ, SP 800-227.

Bottlenecks:

Engineering problems that needed solving

The elephant in the room: Size

- Size: ~ 5 kb keys and signatures are too big.
- DNS and WebPKI are developing Merkle Tree Ladder and Merkle Tree Certificates
- Messagers like iMessage, Signal, MLS typically re-key on every message.
  - but messages can be very short:
    “Hey, u free?”
    “Nice 👍”
    32 bytes of X25519 data on each message is fine. ~ 5 kb of ML-KEM is not.
  - Solution: an “amortized” approach: keep an “inner” X25519 on every message and rekey an “outer” ML-KEM less frequently.

This is all novel cryptography requiring careful design and analysis.

Bickering

A quarrel about petty points

Bickering:
A quarrel about petty points

These are points where either outcome would have been better than delay.

Policy decisions and guidance:

- TLS Ciphersuites: “Recommended: Y / N” for each algorithm.
- Requiring, allowing, or forbidding:
  - Hybrids / Composites vs pure ML-DSA / ML-KEM
  - Private keys as {Seed, Key, Both}
  - Hash-based signatures (particularly LMS)
  - Level 1 (ML-DSA-44) and Level 5 (ML-DSA-87)
- WebPKI: allow ML-DSA roots now, or wait for MTC maturity

Bickering:
A quarrel about petty points

Terminology and definition documents

- “PQ/T Hybrids” – RFC 9794
- “PQC For Engineers” – RFC 9958
- While useful, we *still* waste time arguing *“Post-Quantum”* vs *“Quantum-Safe”*, for example.

Guidance documents

- draft-ietf-pquip-hbs-state
- draft-ietf-pquip-pqc-hsm-constrained
- Trying to get consensus on guidance language is always extremely difficult.

Building Momentum

An opinion or position reached by a group as a whole

Building Momentum:

An opinion or position reached by a group as a whole

The bickering often lead to multiple solutions being standardized.

Now, industry has too many options which delays productization and increases deployment complexity.

We need to push through this!

Building Momentum:

An opinion or position reached by a group as a whole

Seeds were added to FIPS 203 / 204 between ipd and final, rather subtly.

- It took 6 months (Aug 2024 -> Feb 2025) for NIST to clarify officially that they are allowed.
- During that time, hardware products shipped under that initial interpretation. Now we have hardware (and sometimes keys) in production that do not persist their RNG seeds.
- Momentum is building for Seeds as the superior private key format, but we have to wait for that first generation of devices to be updated in order to have full cross-ecosystem support.

Building Momentum:

An opinion or position reached by a group as a whole

Pre-hashed ML-DSA and SLH-DSA modes were also added between idp and final as HashML-DSA and HashSLH-DSA.

- Shortly after publication, the community realized that there is a better way to do pre-hashing for ML-DSA than what was published – the “external mu” mode.
- It took 6 months (Aug 2024 -> Feb 2025) for NIST to clarify officially that external mu ML-DSA is allowed.
- Now we have two different ways to do pre-hashed ML-DSA, with different security and performance properties, creating confusion in industry.

Building Momentum:

An opinion or position reached by a group as a whole

- Too many algorithms to choose from, particularly for signatures:
  - LMS, ML-DSA, SLH-DSA, FN-DSA, each with multiple parameter sets.
  - With hybrids, that multiplies: {MLDSA-44, -65, -87} X {2048, 3072, 4096, P-256, P-384, P-521}.
  - No (reasonable) hw / sw product will support all of them, so now we need to build momentum for the “defaults”.

Summary

PQC deployment has been delayed by:

Bottlenecks, Bickering, and Building Momentum

Summary

PQC deployment has been delayed by:

Bottlenecks, Bickering, and Building Momentum

- We have been anticipating PQC algorithms and re-designing the Internet stack to accept them since ~ 2017.
- **Bottlenecks:** designing novel cryptographic protocols around PQC, which takes time and careful analysis.
- **Bickering:** Everybody has an opinion about PQC policy and guidelines, leads to noisy discussions that take a long time to settle down.
- **Building Momentum:** Now that the PQC standards are (more-or-less) finished, we have to take inventory of what building blocks we have available, and especially where there is more than one standardized way to solve a problem (private key format, pre-hashing, parameter sets). Industry needs to converge on what subset will be supported in products.