Quantum-Resistant Cipher Suites for LAKE

draft-ietf-lake-pqsuites

Version -02

Göran Selander, John Preuß Mattsson, Clément Papon

LAKE WG – IETF 127 – San Francisco – November 20

History

- `draft-spm-lake-pqsuites`: individual draft, -00 (Jul. 2025) → -02 (Apr. 2026)
- Adoption call: June 2026
  https://mailarchive.ietf.org/arch/msg/lake/9Sg048D7wQXKby9yzAC9rVIZ24k/
- Adopted as `draft-ietf-lake-pqsuites` in July 2026
  https://mailarchive.ietf.org/arch/msg/lake/26Q778Wo07dVmBbTALhyaVIWjY0/
- Since then: -00 → -01 → -02 (Nov. 2026)
- Repo moved to the WG: https://github.com/lake-wg/pqsuites

Scope: what the draft does

- **Goal:** new cipher suites for LAKE (RFC 9528) with **ML-KEM** (key exchange) and **ML-DSA** (signatures) to provide post-quantum security
- Covers **Method 0** (signature/signature) and the **PSK** method
  - Methods 1–3 need DH/NIKE → no standard PQ replacement
- **Ephemeral KEM instead of Ephemeral DH:**
  - message_1: G_X carries the Initiator's encapsulation key
  - message_2: the KEM ciphertext replaces G_Y
  - fresh KEM key pair for every session
- **IANA:** new "Requires DH/NIKE" and "Supports DH/NIKE" columns to Method Types and Cipher Suites registries respectively
- Rename EDHOC to LAKE in both the terminology and the registries

Scope: cipher suites

Suite	AEAD	Hash	KEM	Signature	App. AEAD	App. hash
TBD1	AES-CCM-16-128-128	SHAKE256	ML-KEM-512	ML-DSA-44	AES-CCM-16-64-128	SHA-256
TBD2	A256GCM	SHAKE256	ML-KEM-512	ML-DSA-44	A256GCM	SHA-256
TBD3	A256GCM	SHA-384	ML-KEM-1024	ML-DSA-87	A256GCM	SHA-384

- TBD3: high security, aligned with CNSA 2.0 requirements
- KEM ciphertext in message_2: 768 bytes (ML-KEM-512), 1568 bytes (ML-KEM-1024)
- For all three suites: "Supports DH/NIKE" = No

Changes since -00

Issue #5 [1] [2]

- **Application hash clarified**
  - → **Sec. 2:** SHAKE256 is the LAKE hash (used by ML-KEM/ML-DSA); *"as application hash function in these cipher suites, the legacy algorithms SHA-256 or SHA-384 are still used"*
- **Constrained-device limitation stated**
  - → **Sec. 2:** suites may not fit some constrained device classes, due to larger signatures and KEM keys
- **PSK method added to Method Types**
  - → **Sec. 6:** Method Types table now has a PSK row (value 4)

[1] https://github.com/lake-wg/pqsuites/issues/5

[2] https://mailarchive.ietf.org/arch/msg/lake/BH2ugEAuLOiVPVeV5zbNMnXWh78/

Changes since -00

- **Security Considerations section expanded**
  - → **Sec. 4** is now structured in five subsections:
    - 4.1 classical properties of RFC 9528 preserved (Method 0 and PSK)
    - 4.2 existing formal analyses (ROM); QROM (Q1) analysis left as future work
    - 4.2.1 protection against Store-Now-Decrypt-Later attacks
    - 4.2.2 PQ/T hybridization
    - 4.2.3 protection against side-channel attacks

Changes since -00

Issues #15 & #16: rename IANA registries and protocol terms [3] [4]

- **The draft renames the registries and makes clear that the rename also applies to EDHOC Exporter, EDHOC AEAD algorithm, etc.**

  ~~"The EDHOC prefix is retained where needed to avoid ambiguity with terminology and registry entries defined in [RFC9528], for example in the IANA registries."~~

→ **Sec. 1.1:** all 'EDHOC'-prefixed terms become 'LAKE'

→ **Sec. 6:** now includes two more subsections:

- **Sec. 6.1** requires IANA to change the name of the registry group "EDHOC" to "LAKE"
- **Sec. 6.2** lists the "EDHOC"-prefixed terms of registries that are renamed accordingly (**EDHOC** → **LAKE** Cipher Suites, Method Types, etc.)

Impact: names only – no change to registered values or messages

[3] https://mailarchive.ietf.org/arch/msg/lake/ts-czwc4QDolMNWEAUfBBjw1OWQ/

[4] https://mailarchive.ietf.org/arch/msg/lake/0Srz4jSN22m9Av3X4jEdHmRH4eE/

Stephen Farrell's comments on -01

Discussed in [5], [6] and [7]

- **PQ suites increase sizes: is LAKE still worth it vs. (D)TLS?**
  - → Yes – the re-justification mainly concerns new methods, which authkem-edhoc addresses. Estimates with ML-KEM-512 / ML-DSA-44: ≈7.2 kB for DTLS 1.3 vs. ≈3.2 kB for LAKE with KEM-based authentication
  - → This draft gives existing LAKE deployments a PQ migration path, *e.g.*, CNSA 1.0 to CNSA 2.0
  - → A size comparison is useful, but out of scope for this draft

[5] https://mailarchive.ietf.org/arch/msg/lake/oz2sMPz6pitQ4nHpjgTL_4c5szc/

[6] https://mailarchive.ietf.org/arch/msg/lake/lM1DjS6IMkSW1DpfcI5PSn5FMnQ/

[7] https://mailarchive.ietf.org/arch/msg/lake/HGwP-NgpQMMcfvfafDi3tAq6YPA/

Editorial changes

- **Text:**
  - abstract and intro rewritten (Issue #2);
  - "DH/NIKE" properly defined (Issue #12);
  - typos and wording fixes throughout
- **Fix:**
  - TBD3 uses ML-DSA-87 not 85 (Issue #4)
- **IANA section:**
  - proper tables instead of figures (Issue #13);
  - completed instructions, including reserved values (Issue #14)
- **References:**
  - Updated

Next steps

- Waiting for reviews and feedback on version -02
- Ready for WGLC?

Thank you!

Questions & comments

https://github.com/lake-wg/pqsuites

Discussion on PQ/T hybrid algorithms in LAKE cipher suites

PQ/T hybrid cipher suites: what has been said

- **Jun. 2026** – PQ design team → Issue #1 [8]: mention that hybrids could be registered in the future
- **Jul. 2026** – L. Pocero Fraile [9]: mention possible PQ/T hybrid suites against HNDL
- **Aug. 2026** – J. Preuß Mattsson (Issue #1): wait for hybrid KEMs registered in COSE; add a sentence to the draft
- **Sep. 2026** – S. Farrell [10]: define an X25519/ML-KEM hybrid *now* (hard-to-update devices) → [11] and [12]: conclude on a possible algorithm-level hybrid (CFRG KEMs in COSE), not TLS-style; separate document, in parallel
- **In -02:** KEM procedure also applies to hybrid KEMs (**Sec. 3**); hybrids "could be registered in the future" (**Sec. 4.2.2**)

[8] https://github.com/lake-wg/pqsuites/issues/1

[9] https://mailarchive.ietf.org/arch/msg/lake/D5r0X-GKUyQ-X4k8PtJow3rYFxA/

[10] https://mailarchive.ietf.org/arch/msg/lake/oz2sMPz6pitQ4nHpjgTL_4c5szc/

[11] https://mailarchive.ietf.org/arch/msg/lake/lM1DjS6IMkSW1DpfcI5PSn5FMnQ/

[12] https://mailarchive.ietf.org/arch/msg/lake/HGwP-NgpQMMcfvfafDi3tAq6YPA/

PQ/T hybrid cipher suites: way forward?

- **What it would take:**
  - register CFRG hybrid KEMs (e.g. MLKEM768-X25519) as COSE algorithms
  - define LAKE cipher suites using them – the easy part
- **Proposal:** separate document, `pqsuites` proceeds unchanged
- **Dependency:** CFRG hybrid KEM drafts are not finalized yet (RG Last Call ended in July 2026, waiting for revised versions)

Question to the WG: (1) Is there interest in PQ/T hybrid suites for LAKE? (2) If so, OK with a separate document, without delaying `pqsuites`?