

Composite ML-KEM for use in X.509 Public Key Infrastructure

[draft-ietf-lamps-pq-composite-kem-12](#)

Mike Ounsworth, John Gray, Massimiliano Pala, Jan Klaußner, Scott
Fluhrer

IETF 125 – LAMPS

Status

- The WG will recall the kerfuffle between LAMPS and CFRG composite KEM authors about labels just prior to 124 – Montréal.
- Draft has been stable since then.
- We were blocked waiting for a proof-of-security paper

– Published to eprint.iacr.org on 2026-03-05 >



- A few editorial issues open on github.
- @Chairs – have we already done a WGLC?

Paper 2026/427

StarHunters— Secure Hybrid Post-Quantum KEMs From IND-CCA2 PKEs

Deirdre Connolly , Oracle, Selkie Cryptography

Mike Ounsworth , Entrust (Canada)

Sophie Schmieg , Google (United States)

Douglas Stebila , University of Waterloo

Abstract

This paper formally specifies and analyzes the CK hybrid key encapsulation mechanism (KEM) construction from the IDTE CFRG's recent draft on hybrid (post-quantum/traditional) KEMs. CK combines

Composite ML-KEM for use in Cryptographic Message Syntax (CMS)

[draft-ietf-lamps-cms-composite-kem-00](#)

Daniel Van Geest, Mike Ounsworth, John Gray, Jan Klaußner

IETF 125 – LAMPS

What?

- Straightforward application of *draft-ietf-lamps-pq-composite-kem* to CMS

How?

```
cat RFC9936.txt | sed 's/ML-KEM/Composite ML-KEM/g'
```

- **MUST** support (for interop purposes):
 - KEMRecipientInfo.kdf = id-alg-hkdf-with-sha256
 - KEMRecipientInfo.wrap = id-aes256-wrap
- **MAY** use others

Next?

- Tweak references
- Reminder that Composite ML-KEM doesn't use ML-KEM-512
- WGLC?