MLS R. Mahy
Internet-Draft
Intended status: Informational R. L. Barnes
Expires: 3 September 2026 Cisco
2 March 2026

# ML-KEM and Hybrid Cipher Suites for Messaging Layer Security
draft-ietf-mls-pq-ciphersuites-03

## Abstract

This document registers new cipher suites for Messaging Layer Security (MLS) based on "post-quantum" algorithms, which are intended to be resilient to attack by quantum computers. These cipher suites are constructed using the new Module-Lattice Key Encapsulation Mechanism (ML-KEM), optionally in combination with traditional elliptic curve KEMs, together with appropriate authenticated encryption, hash, and signature algorithms.

## About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://mlswg.github.io/mls-pq-ciphersuites/#go.draft-ietf-mls-pq-ciphersuites.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-mls-pq-ciphersuites/.

Discussion of this document takes place on the MLS Working Group mailing list (mailto:mls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/mls/. Subscribe at https://www.ietf.org/mailman/listinfo/mls/.

Source for this draft and an issue tracker can be found at https://github.com/mlswg/mls-pq-ciphersuites/.

## Status of This Memo

## Copyright Notice



## Table of Contents



## 1. Introduction

The potential availability of a cryptographically-relevant quantum computer has caused concern that well-funded adversaries could overturn long-held assumptions about the security assurances of classical Key Exchange Mechanisms (KEMs) and classical cryptographic signatures, which are fundamental to modern security protocols, including the MLS protocol [RFC9420].

Of particular concern are "harvest now, decrypt later" attacks, by which an attacker could collect encrypted traffic now, before a quantum computer exists, and later use a quantum computer to break the confidentiality protections on the collected traffic.

In response to these concerns, the cryptographic community has defined "post-quantum" algorithms, which are designed to be resilient to attacks by quantum computers. Symmetric algorithms can be made post-quantum secure simply by using longer keys and hashes. For asymmetric operations such as KEMs and signatures, entirely new algorithms are needed.

In this document, we define ciphersuites that use the post-quantum secure Module-Lattice-Based KEM (ML-KEM) [MLKEM] together with appropriate symmetric algorithms, and either traditional or Module-Lattice-Based Digital Signature Algorithm (ML-DSA) [MLDSA] post-quantum signature algorithms. The traditional signature cipher suites address the risk of "harvest now, decrypt later" attacks, while not taking on the additional cost of post-quantum signatures. The cipher suites with post-quantum signatures use only post-quantum KEMs.

Following the pattern of base MLS, we define several variations, to allow for users that prefer to only use NIST-approved cryptography, users that prefer a higher security level, and users that prefer a PQ/traditional hybrid KEM over pure ML-KEM:

* ML-KEM-768 + X25519 (128-bit security, Non-NIST, PQ/T hybrid)

* ML-KEM-768 + P-256 (128-bit security, NIST, PQ/T hybrid)

* ML-KEM-1024 + P-384 (192-bit security, NIST, PQ/T hybrid)

* ML-KEM-768 (128-bit security, NIST, pure PQ KEM)

* ML-KEM-1024 (192-bit security, NIST, pure PQ KEM)

* ML-KEM-768 (192-bit security, NIST, pure PQ)

* ML-KEM-1024 (256-bit security, NIST, pure PQ)

Some parts of the community wish to support the 128-bit security level with the same the Authenticated Encryption with Authenticated Data (AEAD) [RFC5116] algorithm and hash function as used in the traditional cipher suites registered in [RFC9420] (AES128 GCM [GCM] and HMAC [RFC2104] with SHA-256 [SHS]), while other parts of the community would like to follow recent recommendations to transition immediately to AES256 GCM [GCM] and HMAC [RFC2104] with SHA-384 [SHS].

For all of the cipher suites defined in this document, we use SHAKE256 (Section 3.2 of [FIPS202]) as the Key Derivation Function (KDF). For the cipher suites at the 192-bit or 256-security levels, we use AES256 GCM [GCM] as the AEAD algorithm, and HMAC [RFC2104] with SHA-384 [SHS] as the hash function.

For the PQ/T hybrid KEMs and the pure ML-KEM HPKE integration, we use the KEMs defined in [I-D.ietf-hpke-pq]. The signature schemes for ML-DSA-65 and ML-DSA-87 [MLDSA] are defined in [I-D.ietf-tls-mldsa].

## 2. IANA Considerations

### 2.1. MLS Cipher Suites

This document requests that IANA add the following entries to the "MLS Cipher Suites" registry, replacing "XXXX" with the RFC number assigned to this document:

| Value | Name | Rec | Reference |
|---|---|---|---|
| TBD1 | MLS_128_MLKEM768X25519_AES128GCM_SHA256_Ed25519 | Y | RFCXXXX |
| TBD2 | MLS_128_MLKEM768X25519_AES256GCM_SHA384_Ed25519 | Y | RFCXXXX |
| TBD3 | MLS_128_MLKEM768P256_AES128GCM_SHA256_P256 | Y | RFCXXXX |
| TBD4 | MLS_128_MLKEM768P256_AES256GCM_SHA384_P256 | Y | RFCXXXX |
| TBD5 | MLS_192_MLKEM1024P384_AES256GCM_SHA384_P384 | Y | RFCXXXX |
| TBD6 | MLS_128_MLKEM768_AES256GCM_SHA384_P256 | Y | RFCXXXX |
| TBD7 | MLS_192_MLKEM1024_AES256GCM_SHA384_P384 | Y | RFCXXXX |
| TBD8 | MLS_192_MLKEM768_AES256GCM_SHA384_MLDSA65 | Y | RFCXXXX |
| TBD9 | MLS_256_MLKEM1024_AES256GCM_SHA384_MLDSA87 | Y | RFCXXXX |

Table 1

The mapping of cipher suites to HPKE primitives [I-D.ietf-hpke-hpke], HMAC hash functions, and TLS signature schemes [RFC8446] is as follows:

| Value | KEM | KDF | AEAD | Hash | Signature |
|---|---|---|---|---|---|
| 0xTBD1 | 0x647a | 0x0011 | 0x0001 | SHA256 | ed25519 |
| 0xTBD2 | 0x647a | 0x0011 | 0x0002 | SHA384 | ed25519 |
| 0xTBD3 | 0x0050 | 0x0011 | 0x0001 | SHA256 | ecdsa_secp256r1_sha256 |
| 0xTBD4 | 0x0050 | 0x0011 | 0x0002 | SHA384 | ecdsa_secp256r1_sha256 |
| 0xTBD5 | 0x0051 | 0x0011 | 0x0002 | SHA384 | ecdsa_secp384r1_sha384 |
| 0xTBD6 | 0x0041 | 0x0011 | 0x0002 | SHA384 | ecdsa_secp256r1_sha256 |
| 0xTBD7 | 0x0042 | 0x0011 | 0x0002 | SHA384 | ecdsa_secp384r1_sha384 |
| 0xTBD8 | 0x0041 | 0x0011 | 0x0002 | SHA384 | mldsa65 |
| 0xTBD9 | 0x0042 | 0x0011 | 0x0002 | SHA384 | mldsa87 |

Table 2

The hash used for the MLS transcript hash is the one referenced in the cipher suite name.  "SHA246" and "SHA384" refer to the SHA-256 and SHA-384 functions defined in [SHS].

## 3.  Security Considerations

The first seven ciphersuites defined in this document combine a post-quantum (or PQ/T hybrid) KEM with a traditional signature algorithm. As such, they are designed to provide confidentiality against quantum and classical attacks, but provide authenticity against classical attacks only.  Thus, these cipher suites do not provide full post-quantum security, only post-quantum confidentiality.

The last two cipher suites also use post-quantum signature algorithms.

For security considerations related to the KEMs used in this document, please see the documents that define those KEMs [I-D.ietf-hpke-pq] and [I-D.irtf-cfrg-hybrid-kems].  For security considerations related to the post-quantum signature algorithms used in this document, please see [I-D.ietf-tls-mldsa] and [I-D.ietf-lamps-dilithium-certificates].

## 4.  References

### 4.1. Normative References

[FIPS202] "SHA-3 standard :: permutation-based hash and extendable-output functions", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.202, 2015, <https://doi.org/10.6028/nist.fips.202>.

[GCM] Dworkin, M., "Recommendation for block cipher modes of operation :: GaloisCounter Mode (GCM) and GMAC", National Institute of Standards and Technology, DOI 10.6028/nist.sp.800-38d, 2007, <https://doi.org/10.6028/nist.sp.800-38d>.

[I-D.ietf-hpke-hpke] Barnes, R., Bhargavan, K., Lipp, B., and C. A. Wood, "Hybrid Public Key Encryption", Work in Progress, Internet-Draft, draft-ietf-hpke-hpke-02, 4 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-hpke-02>.

[I-D.ietf-hpke-pq] Barnes, R. and D. Connolly, "Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE", Work in Progress, Internet-Draft, draft-ietf-hpke-pq-03, 6 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-pq-03>.

[I-D.ietf-tls-mldsa] Hollebeek, T., Schmieg, S., and B. Westerbaan, "Use of ML-DSA in TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-mldsa-01, 26 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-mldsa-01>.

[MLDSA] "Module-lattice-based digital signature standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.204, August 2024, <https://doi.org/10.6028/nist.fips.204>.

[MLKEM] "Module-lattice-based key-encapsulation mechanism standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.203, August 2024, <https://doi.org/10.6028/nist.fips.203>.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/rfc/rfc2104>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <https://www.rfc-editor.org/rfc/rfc5116>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[RFC9420] Barnes, R., Beurdouche, B., Robert, R., Millican, J., Omara, E., and K. Cohn-Gordon, "The Messaging Layer Security (MLS) Protocol", RFC 9420, DOI 10.17487/RFC9420, July 2023, <https://www.rfc-editor.org/rfc/rfc9420>.

[SHS] "Secure hash standard", National Institute of Standards and Technology (U.S.), DOI 10.6028/nist.fips.180-4, 2015, <https://doi.org/10.6028/nist.fips.180-4>.

## 4.2. Informative References

[I-D.ietf-lamps-dilithium-certificates]
Massimo, J., Kampanakis, P., Turner, S., and B. Westerbaan, "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)", Work in Progress, Internet-Draft, draft-ietf-lamps-dilithium-certificates-13, 30 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-dilithium-certificates-13>.

[I-D.irtf-cfrg-hybrid-kems]
Connolly, D., Barnes, R., and P. Grubbs, "Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-hybrid-kems-08, 27 January 2026, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hybrid-kems-08>.

## Acknowledgments

This work would not be possible without the hard work of the CFRG Hybrid KEM design team: Aron Wussler, Bas Westerbaan, Deirdre Connolly, Mike Ounsworth, Nick Sullivan, and Stephen Farrell. Thanks also to Jo谷l Alwen, Marta Mularczyk, and Britta Hale.

## Authors’ Addresses

Rohan Mahy
Email: rohan.ietf@gmail.com

Richard L. Barnes
Cisco
Email: rlb@ipv.sx