LAKE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 21 October 2026

G. Selander
J. Preu Mattsson
Ericsson

19 April 2026

Quantum-Resistant Cipher Suites for EDHOC
draft-spm-lake-pqsuites-02

Abstract

The Lightweight Authenticated Key Exchange (LAKE) protocol, Ephemeral Diffie-Hellman over COSE (EDHOC), achieves post-quantum security by adding new cipher suites with quantum-resistant algorithms, such as ML-DSA for digital signatures and ML-KEM for key exchange. This document specifies how EDHOC operates in a post-quantum setting using both signature-based and PSK-based authentication methods, and defines corresponding cipher suites.

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-spm-lake-pqsuites/.

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

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

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

The Lightweight Authenticated Key Exchange (LAKE) protocol, Ephemeral Diffie-Hellman over COSE (EDHOC) [RFC9528], supports the use of multiple authentication methods and the negotiation of cipher suites based on COSE algorithms. Currently, four asymmetric authentication methods (0, 1, 2, and 3) are defined. In addition, a symmetric key-based authentication method is being developed, see [I-D.ietf-lake-edhoc-psk].

Currently defined cipher suites rely on Elliptic Curve Cryptography (ECC) for key exchange and authentication, making them vulnerable in the event that a Cryptographically Relevant Quantum Computer (CRQC) is constructed.

This document specifies how EDHOC can operate in a post-quantum setting using both signature-based and PSK-based authentication, and defines corresponding cipher suites.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Readers are expected to be familiar with EDHOC [RFC9528].

2. EDHOC with Quantum-Resistant Algorithms

Method 0 in [RFC9528], which uses digital signatures for authentication by both the Initiator and Responder, and also the PSK method in [I-D.ietf-lake-edhoc-psk], is straightforward to use with standardized post-quantum algorithms.

A quantum-resistant signature algorithm, such as ML-DSA [I-D.ietf-cose-dilithium], is a drop-in replacement for classical signature algorithms such as ECDSA. For post-quantum secure key exchange, a quantum-resistant Key Encapsulation Mechanism (KEM), such as ML-KEM [I-D.ietf-jose-pqc-kem], can be applied directly to EDHOC, as is detailed in Section 3.

To enable post-quantum security in EDHOC it suffices to register new cipher suites using COSE registered algorithms. Cipher suites using ML-KEM-512 [I-D.ietf-jose-pqc-kem] for key exchange and ML-DSA-44 [I-D.ietf-cose-dilithium] for digital signatures are specified in Section 6.2. As both ML-KEM [FIPS203] and ML-DSA [FIPS204] internally use SHAKE256, it is natural to also use SHAKE256 for EDHOC’s key derivation. Additional post-quantum cipher suites may be specified.

Methods 13 in [RFC9528] use a Diffie-Hellman/Non-Interactive Key Exchange (NIKE) based API for authentication. As of this writing, no standardized post-quantum algorithms for these methods exist. To highlight which methods that require DH/NIKE a column is added to the EDHOC Method Type registry, see Section 6.1. To highlight matching cipher suites a corresponding column indicating support for DH/NIKE is added, see Section 6.2.

An alternative path to post-quantum EDHOC, not pursued in this document, would be to define new authentication methods based on Key Encapsulation Mechanisms (KEMs).

Compared to elliptic curve algorithms such as ECDHE, ECDSA, and EdDSA, ML-KEM-512 and ML-DSA-44 introduce significantly higher overhead [FIPS203][FIPS204]. More efficient post-quantum signature schemes are being standardized, such as FN-DSA.

3. Using KEMs in EDHOC Key Exchange

Given a quantum-resistant KEM, such as ML-KEM-512, with encapsulation key ek, ciphertext c, and shared secret key K (using the notation of [FIPS203]). The Diffie-Hellman procedure in EDHOC is replaced by a KEM procedure as follows:

* The Initiator generates a new encapsulation / decapsulation key pair matching the selected cipher suite.

* The encapsulation key ek is transported in the G_X field in message_1.

* The Responder calculates (K,c) = Encaps(ek).

* The ciphertext c is transported in the G_Y field in message_2.

* The Initiator calculates the shared secret K = Decaps(c).

* G_XY is the shared secret key K.

The security requirements and security considerations of EDHOC and the KEM algorithm used apply. For example, the Initiator MUST generate a new encapsulation / decapsulation key pair for each EDHOC session.

Note that G_Y does not contain a public key when a KEM is used in this way. The definition of EDHOC message_2 in Section 5.3.1 of [RFC9528] remains the same:

```
message_2 = (
  G_Y_CIPHERTEXT_2 : bstr,
)
```

and G_Y_CIPHERTEXT_2 remains the concatenation of G_Y and CIPHERTEXT_2, the latter is defined in Section 5.3.2 of [RFC9528]. But now G_Y is a KEM ciphertext.

Just as with the ephemeral key G_Y, the length of KEM ciphertext G_Y is known from the corresponding algorithm in the selected cipher suite, see Figure 1. Hence the Initator can separate out the concatenated ciphertexts and decapsulate and decrypt, respectively.

KEM	Length of ciphertext (bytes)
ML-KEM-512	768
ML-KEM-768	1088
ML-KEM-1024	1568

Figure 1: Length of ML-KEM Ciphertext.

Note also that this use of KEM applies both to standalone KEM and hybrid KEMs such as, e.g., X-wing [I-D.connolly-cfrg-xwing-kem].

Conventions for using post-quantum KEMs within COSE are described in [I-D.ietf-jose-pqc-kem]. The shared secret key K corresponds to the initial shared secret SS’ in that document.

4. Security Considerations

The cipher suites defined in [RFC9528] rely on Elliptic Curve Cryptography (ECC) for key exchange and authentication, which would be broken by a Cryptographically Relevant Quantum Computer (CRQC). In contrast, the cipher suites specified in this document use the quantum-resistant algorithms ML-KEM for key exchange and ML-DSA for authentication. When used with Method 0 from [RFC9528], where both the Initiator and Responder authenticate using digital signatures, or with the PSK method defined in [I-D.ietf-lake-edhoc-psk], these cipher suites preserve the same security properties even in the presence of a quantum-capable adversary.

Security considerations of ML-KEM are discussed in [I-D.sfluhrer-cfrg-ml-kem-security-considerations].

5. Privacy Considerations

TBD

6. IANA Considerations

6.1. EDHOC Method Type Registry

IANA is requested to update the EDHOC Method Type registry with a column with heading "Requires DH/NIKE" indicating that the method requires Diffie-Hellman or Non-Interactive Key Exchange. Valid table entries in this column are "Yes" and "No".

For the existing Method Types, the following entries are inserted in the new "Requires DH/NIKE" column:

Value: 0, Requires DH/NIKE: No
Value: 1, Requires DH/NIKE: Yes
Value: 2, Requires DH/NIKE: Yes
Value: 3, Requires DH/NIKE: Yes

6.2. EDHOC Cipher Suites Registry

IANA is requested to update the EDHOC Cipher Suites registry with a column with heading "Supports DH/NIKE" indicating that the cipher suite supports Diffie-Hellman or Non-Interactive Key Exchange. Valid table entries in this column are "Yes" and "No".

For the existing EDHOC Cipher Suites 0-6, 24, 25, the entry "Yes" is inserted in the new "Supports DH/NIKE" column.

Furthermore, IANA is requested to register the following entries in the EDHOC Cipher Suites Registry:

Value: TBD1
Array: 30, -45, 16, TBD10, -48, 10, -16
Description: AES-CCM-16-128-128, SHAKE256, 16, MLKEM512, ML-DSA-44, AES-CCM-16-64-128, SHA-256
Supports DH/NIKE: No
Reference: [[This document]]

Value: TBD2
Array: 3, -45, 16, TBD10, -48, 3, -16
Description: A256GCM, SHAKE256, 16, MLKEM512, ML-DSA-44, A256GCM, SHA-256
Supports DH/NIKE: No
Reference: [[This document]]

Value: TBD3
Array: 3, -43, 16, TBD12, -48, 3, -43
Description: A256GCM, SHA-384, 16, MLKEM1024, ML-DSA-85,
A256GCM, SHA-384
Supports DH/NIKE: No
Reference: [[This document]]

Cipher suite TBD3 is intended for for high security applications such as government use and financial applications. This cipher suites consists of algorithms from the Commercial National Security Algorithm (CNSA) 2.0 suite [CNSA2].

7. References

7.1. Normative References

[I-D.ietf-cose-dilithium]
Prorock, M. and O. Steele, "ML-DSA for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-cose-dilithium-11, 15 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-dilithium-11>.

[I-D.ietf-jose-pqc-kem]
Reddy.K, T., Banerjee, A., and H. Tschofenig, "Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-jose-pqc-kem-05, 8 December 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-jose-pqc-kem-05>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9528] Selander, G., Preu Mattsson, J., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", RFC 9528, DOI 10.17487/RFC9528, March 2024, <https://www.rfc-editor.org/rfc/rfc9528>.

7.2. Informative References

[FIPS203] "Module-Lattice-Based Key-Encapsulation Mechanism Standard", NIST FIPS 203, August 2024, <https://doi.org/10.6028/NIST.FIPS.203>.

[FIPS204] "Module-Lattice-Based Digital Signature Standard", NIST FIPS 204, August 2024, <https://doi.org/10.6028/NIST.FIPS.204>.

[I-D.connolly-cfrg-xwing-kem] Connolly, D., Schwabe, P., and B. Westerbaan, "X-Wing: general-purpose hybrid post-quantum KEM", Work in Progress, Internet-Draft, draft-connolly-cfrg-xwing-kem-10, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-connolly-cfrg-xwing-kem-10>.

[I-D.ietf-lake-edhoc-psk] Lopez-Perez, Selander, G., Mattsson, J. P., Marin-Lopez, R., and F. Lopez-Gomez, "EDHOC Authenticated with Pre-Shared Keys (PSK)", Work in Progress, Internet-Draft, draft-ietf-lake-edhoc-psk-07, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-lake-edhoc-psk-07>.

[I-D.sfluhrer-cfrg-ml-kem-security-considerations] Fluhrer, S., Dang, Q., Mattsson, J. P., Milner, K., and D. Shiu, "ML-KEM Security Considerations", Work in Progress, Internet-Draft, draft-sfluhrer-cfrg-ml-kem-security-considerations-04, 17 November 2025, <https://datatracker.ietf.org/doc/html/draft-sfluhrer-cfrg-ml-kem-security-considerations-04>.

Acknowledgments

This work was supported partially by Vinnova - the Swedish Agency for Innovation Systems - through the EUREKA CELTIC-NEXT project CYPRESS.

Authors' Addresses

Gran Selander
Ericsson
Email: goran.selander@ericsson.com

John Preu Mattsson
Ericsson
Email: john.mattsson@ericsson.com