COSE
Internet-Draft
Intended status: Standards Track
Expires: 8 January 2026

T. Reddy
Nokia
H. Tschofenig
7 July 2025

PQ/T Hybrid KEM: HPKE with JOSE/COSE
draft-reddy-cose-jose-pqc-hybrid-hpke-08

Abstract

This document outlines the construction of a PQ/T Hybrid Key Encapsulation Mechanism (KEM) in Hybrid Public-Key Encryption (HPKE) for integration with JOSE and COSE. It specifies the utilization of both traditional and Post-Quantum Cryptography (PQC) algorithms, referred to as PQ/T Hybrid KEM, within the context of JOSE and COSE.

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-reddy-cose-jose-pqc-hybrid/.

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

Status of This Memo

Table of Contents

1. Introduction

The migration to Post-Quantum Cryptography (PQC) is unique in the history of modern digital cryptography in that neither the traditional algorithms nor the post-quantum algorithms are fully trusted to protect data for the required data lifetimes. The traditional algorithms, such as RSA and elliptic curve, will fall to quantum cryptalanysis, while the post-quantum algorithms face uncertainty about the underlying mathematics, compliance issues, unknown vulnerabilities, hardware and software implementations that have not had sufficient maturing time to rule out classical cryptanalytic attacks and implementation bugs.

During the transition from traditional to post-quantum algorithms, there is a desire or a requirement for protocols that use both algorithm types. Hybrid key exchange refers to using multiple key exchange algorithms simultaneously and combining the result with the goal of providing security even if all but one of the component algorithms is broken. It is motivated by transition to post-quantum cryptography.

HPKE offers a variant of public-key encryption of arbitrary-sized plaintexts for a recipient public key. The specifications for the use of HPKE with JOSE and COSE are described in [I-D.ietf-jose-hpke-encrypt] and [I-D.ietf-cose-hpke], respectively. HPKE can be extended to support PQ/T Hybrid KEM as defined in [I-D.ietf-hpke-pq]. This specification defines PQ/T Hybrid KEM in HPKE for use with JOSE and COSE.

2. Conventions and Definitions

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.

This document makes use of the terms defined in [I-D.ietf-pquip-pqt-hybrid-terminology]. For the purposes of this document, it is helpful to be able to divide cryptographic algorithms into two classes:

"Traditional Algorithm": An asymmetric cryptographic algorithm based on integer factorisation, finite field discrete logarithms, elliptic curve discrete logarithms, or related mathematical problems. In the context of JOSE, examples of traditional key exchange algorithms include Elliptic Curve Diffie-Hellman Ephemeral Static [RFC6090] [RFC8037]. In the context of COSE, examples of traditional key exchange algorithms include Ephemeral-Static (ES) DH and Static-Static (SS) DH [RFC9052].

"Post-Quantum Algorithm": An asymmetric cryptographic algorithm that is believed to be secure against attacks using quantum computers as well as classical computers. Examples of PQC key exchange algorithms include ML-KEM.

"Post-Quantum Traditional (PQ/T) Hybrid Scheme": A multi-algorithm scheme where at least one component algorithm is a post-quantum algorithm and at least one is a traditional algorithm.

"PQ/T Hybrid Key Encapsulation Mechanism": A multi-algorithm KEM made up of two or more component KEM algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.

3. Construction

ML-KEM is a one-pass (store-and-forward) cryptographic mechanism for an originator to securely send keying material to a recipient using the recipient’s ML-KEM public key. Three parameters sets for ML-KEMs are specified by [FIPS203]. In order of increasing security strength (and decreasing performance), these parameter sets are ML-KEM-512, ML-KEM-768, and ML-KEM-1024. PQ/T algorithms for HPKE [I-D.ietf-hpke-pq] uses a multi-algorithm scheme, where one component algorithm is a post-quantum algorithm and another one is a traditional algorithm. The QSF combiner functions defined in Sections 6.1, 6.2 and 6.3 of [I-D.irtf-cfrg-hybrid-kems] combines the output of a post-quantum KEM and a traditional KEM to generate a single shared secret.

4. Ciphersuite Registration

This specification registers a number of PQ/T Hybrid KEMs for use with HPKE. A ciphersuite is thereby a combination of several algorithm configurations:

* KEM algorithm (PQ KEM + Traditional Algorithm, for example, MLKEM768 + X25519 defined as "X25519-MLKEM768-SHAKE256-SHA3256" in [I-D.ietf-hpke-pq])

* KDF algorithm

* AEAD algorithm

The "KEM", "KDF", and "AEAD" values are conceptually taken from the HPKE IANA registry [HPKE-IANA]. Hence, JOSE and COSE cannot use an algorithm combination that is not already available with HPKE.

The HPKE PQ/T hybrid ciphersuites for JOSE and COSE are defined in Section 7. Note that the PQ/T Hybrid KEM in HPKE is not an authenticated KEM. The HPKE Base mode can only be supported with the PQ/T Hybrid KEM.

5. AKP Key for PQ/T Hybrid Algorithms in HPKE

This section describes the required parameters for an "AKP" key type, as defined in [I-D.ietf-cose-dilithium], and its use with the PQ/T Hybrid Algorithms for HPKE, as defined in {#XWING}. An example JWK is also provided for illustration.

5.1. Required Parameters

A JSON Web Key (JWK) or COSE_Key with a key type ("kty") for use with the PQ/T Hybrid Algorithm for HPKE includes the following parameters:

* kty (Key Type)
  The key type parameter MUST be present and set to "AKP".

* alg (Algorithm)
  The algorithm parameter MUST be present and MUST represent the PQ/T algorithm for HPKE, as defined in {#XWING}. PQ/T algorithms for HPKE are those registered in the "JSON Web Signature and Encryption Algorithms" and "COSE Algorithms" registries, derived from the KEM identifier in the HPKE IANA registry.

* pub (Public Key)
  The public key parameter MUST be present and MUST contain the public encapsulation key (pk) as defined in Section 5.1 of [I-D.irtf-cfrg-hybrid-kems]. When represented as a JWK, this value MUST be base64url-encoded.

* priv (Private Key)
  When representing an private key, the private key parameter MUST be present and MUST contain the private decapsulation key (sk) as defined in Section 5.1 of [I-D.irtf-cfrg-hybrid-kems]. When represented as a JWK, this value MUST be base64url-encoded.

5.1.1. Example

The following is an example JWK representation of an "AKP" key for the "QSF-X25519-MLKEM768-SHAKE256-SHA3256" algorithm:

```
{
    "kty"  : "AKP",
    "alg"  : "HPKE-7",
    "pub"  : "4iNrNajCSz...tmrrIzQSQQO9lNA",
    "priv" : "f5wrpOiP...rPpm7yY"
}
```

6. Security Considerations

The security considerations in [I-D.ietf-hpke-pq], [I-D.ietf-jose-hpke-encrypt] and [I-D.ietf-cose-hpke] are to be taken into account.

The shared secrets computed in the hybrid key exchange should be computed in a way that achieves the "hybrid" property: the resulting secret is secure as long as at least one of the component key

exchange algorithms is unbroken. PQC KEMs used in the manner described in this document MUST explicitly be designed to be secure in the event that the public key is reused, such as achieving IND-CCA2 security. ML-KEM has such security properties.

6.1. Post-Quantum Security for Multiple Recipients

In HPKE JWE Key Encryption, when encrypting the Content Encryption Key (CEK) for multiple recipients, it is crucial to consider the security requirements of the message to safeguard against "Harvest Now, Decrypt Later" attack. For messages requiring post-quantum security, all recipients MUST use algorithms supporting post-quantum cryptographic methods, such as PQC KEMs or Hybrid PQ/T KEMs. Using traditional algorithms (e.g., ECDH-ES) for any recipient in these scenarios compromises the overall security of the message.

7. IANA Considerations

7.1. JOSE

This document requests IANA to add new values to the "JSON Web Signature and Encryption Algorithms" registry.

7.1.1. JOSE Algorithms Registry

* Algorithm Name: HPKE-7
* Algorithm Description: Cipher suite for JOSE-HPKE in Base Mode that uses the P-256 + ML-KEM-768 Hybrid KEM, the SHAKE256 KDF, and the AES-256-GCM AEAD.
* Algorithm Usage Location(s): "alg"
* JOSE Implementation Requirements: Optional
* Change Controller: IANA
* Specification Document(s): [[TBD: This RFC]]
* Algorithm Analysis Documents(s): TODO
* Algorithm Name: HPKE-8
* Algorithm Description: Cipher suite for JOSE-HPKE in Base Mode that uses the P-256 + ML-KEM-768 Hybrid KEM, the SHAKE256 KDF, and the ChaCha20Poly1305 AEAD.
* Algorithm Usage Location(s): "alg"

* JOSE Implementation Requirements: Optional

* Change Controller: IANA

* Specification Document(s): [[TBD: This RFC]]

* Algorithm Analysis Documents(s): TODO

* Algorithm Name: HPKE-9

* Algorithm Description: Cipher suite for JOSE-HPKE in Base Mode that uses the X25519 + ML-KEM-768 Hybrid KEM, the SHAKE256 KDF, and the AES-256-GCM AEAD.

* Algorithm Usage Location(s): "alg"

* JOSE Implementation Requirements: Optional

* Change Controller: IANA

* Specification Document(s): [[TBD: This RFC]]

* Algorithm Analysis Documents(s): TODO

* Algorithm Name: HPKE-10

* Algorithm Description: Cipher suite for JOSE-HPKE in Base Mode that uses the X25519 + ML-KEM-768 Hybrid KEM, the SHAKE256 KDF, and the ChaCha20Poly1305 AEAD.

* Algorithm Usage Location(s): "alg"

* JOSE Implementation Requirements: Optional

* Change Controller: IANA

* Specification Document(s): [[TBD: This RFC]]

* Algorithm Analysis Documents(s): TODO

* Algorithm Name: HPKE-11

* Algorithm Description: Cipher suite for JOSE-HPKE in Base Mode that uses the P-384 + ML-KEM-1024 Hybrid KEM, the SHAKE256 KDF, and the AES-256-GCM AEAD.

* Algorithm Usage Location(s): "alg"

* JOSE Implementation Requirements: Optional

* Change Controller: IANA

* Specification Document(s): [[TBD: This RFC]]

* Algorithm Analysis Documents(s): TODO

* Algorithm Name: HPKE-12

* Algorithm Description: Cipher suite for JOSE-HPKE in Base Mode that uses the P-384 + ML-KEM-1024 Hybrid KEM, the SHAKE256 KDF, and the ChaCha20Poly1305 AEAD.

* Algorithm Usage Location(s): "alg"

* JOSE Implementation Requirements: Optional

* Change Controller: IANA

* Specification Document(s): [[TBD: This RFC]]

* Algorithm Analysis Documents(s): TODO

7.2. COSE

This document requests IANA to add new values to the 'COSE Algorithms' registry.

7.2.1. COSE Algorithms Registry

* Name: QSF-P256-MLKEM768-SHAKE256-SHA3256-AES-256-GCM

* Value: TBD1

* Description: Cipher suite for COSE-HPKE in Base Mode that uses the P-256 + ML-KEM-768 Hybrid KEM, the SHAKE256 KDF, and the AES-256-GCM AEAD.

* Capabilities: [kty]

* Change Controller: IANA

* Reference: [[TBD: This RFC]]

* Name: QSF-P256-MLKEM768-SHAKE256-SHA3256-ChaCha20Poly1305

* Value: TBD2

* Description: Cipher suite for COSE-HPKE in Base Mode that uses the P-256 + ML-KEM-768 Hybrid KEM, the SHAKE256 KDF, and the ChaCha20Poly1305 AEAD.

* Capabilities: [kty]

* Change Controller: IANA

* Reference: [[TBD: This RFC]]

* Name: QSF-X25519-MLKEM768-SHAKE256-SHA3256-AES-256-GCM

* Value: TBD3

* Description: Cipher suite for COSE-HPKE in Base Mode that uses the X25519 + ML-KEM-768 Hybrid KEM, the SHAKE256 KDF, and the AES-256-GCM AEAD.

* Capabilities: [kty]

* Change Controller: IANA

* Reference: [[TBD: This RFC]]

* Name: QSF-X25519-MLKEM768-SHAKE256-SHA3256-ChaCha20Poly1305

* Value: TBD4

* Description: Cipher suite for COSE-HPKE in Base Mode that uses the X25519 + ML-KEM-768 Hybrid KEM, the SHAKE256 KDF, and the ChaCha20Poly1305 AEAD.

* Capabilities: [kty]

* Change Controller: IANA

* Reference: [[TBD: This RFC]]

* Name: QSF-P384-MLKEM1024-SHAKE256-SHA3256-AES-256-GCM

* Value: TBD5

* Description: Cipher suite for COSE-HPKE in Base Mode that uses the P-384 + ML-KEM-1024 Hybrid KEM, the SHAKE256 KDF, and the AES-256-GCM AEAD.

* Capabilities: [kty]

* Change Controller: IANA

* Reference: [[TBD: This RFC]]

* Name: QSF-P384-MLKEM1024-SHAKE256-SHA3256-ChaCha20Poly1305

* Value: TBD6

* Description: Cipher suite for COSE-HPKE in Base Mode that uses the P-384 + ML-KEM-1024 Hybrid KEM, the SHAKE256 KDF, and the ChaCha20Poly1305 AEAD.

* Capabilities: [kty]

* Change Controller: IANA

* Reference: [[TBD: This RFC]]

Acknowledgments

Thanks to Ilari Liusvaara and Orie Steele for the discussion and comments.

References

Normative References

[I-D.ietf-cose-dilithium] Prorock, M., Steele, O., Misoczki, R., Osborne, M., and C. Cloostermans, "ML-DSA for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-cose-dilithium-07, 12 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-dilithium-07>.

[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>.

Informative References

[FIPS203] "Module-Lattice-based Key-Encapsulation Mechanism Standard", <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf>.

[HPKE-IANA]
IANA, "Hybrid Public Key Encryption (HPKE) IANA Registry", <https://www.iana.org/assignments/hpke/hpke.xhtml>.

[I-D.ietf-cose-hpke]
Tschofenig, H., Steele, O., Daisuke, A., and L. Lundblade, "Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)", Work in Progress, Internet-Draft, draft-ietf-cose-hpke-13, 4 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-hpke-13>.

[I-D.ietf-hpke-pq]
Barnes, R., "Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE", Work in Progress, Internet-Draft, draft-ietf-hpke-pq-01, 30 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-pq-01>.

[I-D.ietf-jose-hpke-encrypt]
Reddy.K, T., Tschofenig, H., Banerjee, A., Steele, O., and M. B. Jones, "Use of Hybrid Public Key Encryption (HPKE) with JSON Object Signing and Encryption (JOSE)", Work in Progress, Internet-Draft, draft-ietf-jose-hpke-encrypt-10, 20 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-jose-hpke-encrypt-10>.

[I-D.ietf-pquip-pqt-hybrid-terminology]
D, F., P, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", Work in Progress, Internet-Draft, draft-ietf-pquip-pqt-hybrid-terminology-06, 10 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqt-hybrid-terminology-06>.

[I-D.irtf-cfrg-hybrid-kems]
Connolly, D., "Hybrid PQ/T Key Encapsulation Mechanisms", Work in Progress, Internet-Draft, draft-irtf-cfrg-hybrid-kems-03, 25 February 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-hybrid-kems-03>.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, DOI 10.17487/RFC6090, February 2011, <https://www.rfc-editor.org/rfc/rfc6090>.

[RFC8037] Liusvaara, I., "CFRG Elliptic Curve Diffie-Hellman (ECDH) and Signatures in JSON Object Signing and Encryption (JOSE)", RFC 8037, DOI 10.17487/RFC8037, January 2017, <https://www.rfc-editor.org/rfc/rfc8037>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

Authors' Addresses

Tirumaleswar Reddy
Nokia
Bangalore
Karnataka
India
Email: k.tirumaleswar_reddy@nokia.com

Hannes Tschofenig
Germany
Email: hannes.tschofenig@gmx.net