Hybrid key exchange in JOSE and COSE

draft-ra-cose-hybrid-encrypt-02

IETF 118, 07th Nov 2023

Aritra Banerjee (Nokia)

Tiru Reddy (Nokia)

Problem

- 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

- Motivated by the transition to post-quantum cryptography.

- This document provides a construction for hybrid key exchange in JOSE and COSE.

- *This draft defines for both COSE and JOSE , and the COSE based version aligns with JOSE*

Overview

- Hybrid Shared secret (PQC + Traditional)

- Concatenate and Hash approach

- The specification uses the KEM combiner defined in draft-ounsworth-cfrg-kem-combiners-04 that takes in two or more shared secrets and returns a combined shared secret.

- At least one KEM must be IND-CCA2 secure.

KEM

- A KEM is defined as follows
  - ➢def kemKeyGen() -> (pk, sk)
  - ➢def kemEncaps(pk) -> (ct, ss)
  - ➢def kemDecaps(ct, sk) -> ss

- where pk is public key, sk is secret key, ct is the ciphertext representing an encapsulated key, and ss is shared secret.

KMAC functions for each PQ/T Hybrid

PQ/T Hybrid	KDF
x25519-ES_kyber512	KMAC256
secp384r1-ES_kyber768	KMAC256
x25519-ES_kyber768	KMAC256
secp256r1-ES_kyber512	KMAC256

KMAC function

- KMAC is defined in NIST SP 800-56Cr2 [SP800-56C].

- The KMAC(K, X, L, S) parameters are instantiated as follows:

  - K: context-specific string. In case of COSE, the context-specific string will be set to *concat("COSE_PostQuantum_Traditional_Hybrid", "_"*, Name of the PQ/T hybrid algorithm).

    - For example, concat(”COSE_PostQuantum_Traditional_Hybrid", "_", "x25519-ES_kyber512") = ”COSE_PostQuantum_Traditional_Hybrid_x25519-ES_kyber512".

KMAC function (Cont.)

- X: concat(0x00000001, k_1, ... , k_n, fixedInfo). The fixedInfo parameter is a fixed-format string containing *COSE/JOSE* context-specific information.

- L: length of the output key in bits.

- S: utf-8 string "KDF".

Maximum size of K (salt)

- The suggested maximum byte length of K (salt) can be 132 bytes, and the salt can be a multiple of 132 bytes as discussed in Table 3 of [SP800-56C]. However, in this document, K is of variable length.

- The size of "K" will change based on the PQ/T hybrid algorithm.
  - A shorter key K will be padded by appending an all zero-bit string to obtain a 132-byte output.

KEM Combiner Example

Traditional Part

- Shared secret (ss) = KMAC256("COSE_PostQuantum_Traditional_Hybrid_X25519-ES_kyber512", "0x00000001 || HKDF-256(DH-Shared-Secret, salt, context) || ct_1 || rlen(ct_1) || ss_1 || rlen(ss_1) || context" , 256, "KDF")

PQC Part

- Where ss_1 is shared secret and its corresponding ciphertext ct_1 generated from kemEncaps(pk). If ss_1 or ct_1 are not guaranteed to have constant length, rlen encoded length is appended when concatenating as discussed in Section 3.2 of draft-ounsworth-cfrg-kem-combiners-04

Acknowledgement of the HPKE-COSE draft

- The authors acknowledge the presence of the HPKE-COSE draft.
- This draft focusses more on the Traditional (ECDH-ES) + PQC key exchange hybrids and not for the authenticated modes in HPKE for KEMs, KDFs and AADs
- The main goal of this draft is aimed and specifiying a Traditional + PQC hybrid key exchange method for COSE for attacks from a CRQC as well as a traditional computer.
- It leverages existing Traditional (ECDH-ES) and PQC KEM, and combines the shared secret.
- The use of the word "Hybrid" in this draft is different than that of HPKE-COSE and more in line with draft-ietf-tls-hybrid-design, draft-ietf-lamps-composite-kem, draft-wussler-openpgp-pqc

draft-ra-cose-hybrid-encrypt-02

- Comments and suggestions are welcome