Post-quantum Hybrid Key Exchange in the IKEv2 with ECDH, ML-KEM, and FrodoKEM

IETF 120, IPSECME

Guilin Wang

Wang.guilin@Huawei.com

IKEv2 with FrodoKEM

❑ Information of our daft

- **Title**: Post-quantum Hybrid Key Exchange in the IKEv2 with ECDH, ML-KEM, and FrodoKEM (draft-wang-hybrid-kem-ikev2-frodo-01)
- **Author**: Guilin Wang
- **Dates submitted**: v00 on 2024-04-08; v01 on 2024-05-08
- https://datatracker.ietf.org/doc/draft-wang-hybrid-kem-ikev2-frodo/

❑ General Motivation

- The cryptographic agility of PQ migration has been highlighted by many organizations, like NIST, ETSI, BSI. (see talks at ETSI QSC workshop, May of 2024)
- Algorithm diversity is important to support cryptographic agility
- The availability of various PQC algorithms is beneficial to applications
- Generally speaking, post-quantum algorithms are still not mature yet
- Supporting a good size of various algorithms is also good from engineering aspect

IKEv2 with FrodoKEM

❑Concrete Motivation of this draft

- RFC 9370 specifies a framework that supports up to 7 layers of additional KEMs in IEKv2
- [I-D.KR24] by Panos and Gerardo describes how the framework can be run with ML-KEM (Kyber)
- Some applications demanding high security level may need additional PQ KEMs.
- Based on unstructured lattice based KEM, the security of FrodoKEM more conservative, compared to ML-KEM
- **FrodoKEM** is one of three KEMs in the process of ISO standardization

[**I-D.KR24]** Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)
draft-kampanakis-ml-kem-ikev2-03
https://datatracker.ietf.org/doc/draft-kampanakis-ml-kem-ikev2/

IKEv2 with FrodoKEM: Challenges

- **Communication**: The public key and ciphertext of FrodoKEM is about 10 times of ML-KEM
- Luckily, the IKE Intermediate Exchange supports large message exchange (but less than 2^{16} - 1 = 65,535 Bytes) (RFC 9242, RFC 7383)
- Also, need 8 or 12 OIDs: Most likely, ISO shall go for 8 parameter sets

Algorithms	secret key sk	public key pk	ciphterext ct	shared secret ss
ML-KEM-512	800	1,632	768	32
ML-KEM-768	1,184	2,400	1,088	32
ML-KEM-1024	1,568	3,168	1,568	32
FrodoKEM-640	19,888	9,616	9,752	16
FrodoKEM-976	31,296	15,632	15,792	24
FrodoKEM-1344	43,088	21,520	21,696	32

Table 1: Size (in bytes) of keys and ciphertexts of ML-KEM and FrodoKEM

IKEv2 with FrodoKEM: An example

```
Initiator                    Responder
-------------------------------------------------------------------
HDR(IKE_SA_INIT), SAi1(.. ADDKE*...), --->
KEi(Curve25519), Ni, N(IKEV2_FRAG_SUPPORTED),
N(INTERMEDIATE_EXCHANGE_SUPPORTED)
    Proposal #1
    Transform ECR (ID = ENCR_AES_GCM_16,
                   256-bit key)
    Transform PRF (ID = PRF_HMAC_SHA2_512)
    Transform KE (ID = Curve25519)
    Transform ADDKE1 (ID = TBD36)
    Transform ADDKE1 (ID = TBD37)
    Transform ADDKE1 (ID = NONE)
    Transform ADDKE2 (ID = TBD43)
    Transform ADDKE2 (ID = TBD45)
    Transform ADDKE2 (ID = NONE)
    Transform ADDKE3 (ID = TBD49)
    Transform ADDKE3 (ID = NONE)
                                                <--- HDR(IKE_SA_INIT), SAr1(.. ADDKE*...),
                                                     KEr(Curve25519), Nr, N(IKEV2_FRAG_SUPPORTED)
                                                     N(INTERMEDIATE_EXCHANGE_SUPPORTED)
                                                     Proposal #1
                                                       Transform ECR (ID = ENCR_AES_GCM_16,
                                                                      256-bit key)
                                                       Transform PRF (ID = PRF_HMAC_SHA2_512)
                                                       Transform KE (ID = Curve25519)
                                                       Transform ADDKE1 (ID = TBD36)
                                                       Transform ADDKE2 (ID = TBD43)
                                                       Transform ADDKE3 (ID = NONE)
HDR(IKE_INTERMEDIATE), SK {KEi(1)(TBD36)} -->
                        <--- HDR(IKE_INTERMEDIATE), SK {KEr(1)(TBD36)}
HDR(IKE_INTERMEDIATE), SK {KEi(2)(TBD43)} -->
                        <--- HDR(IKE_INTERMEDIATE), SK {KEr(2)(TBD43)}

HDR(IKE_AUTH), SK{ IDi, AUTH, SAi2, TSi, TSr } --->
                           <--- HDR(IKE_AUTH), SK{IDr, AUTH, SAr2,TSi, TSr}
```

IKEv2 with FrodoKEM: Comments

Comments by Leonie Bruckert, 15 May 2024

I really appreciate the intention to use FrodoKEM in IKEv2. However, I do not understand why the draft describes the combination of FrodoKEM and ML-KEM instead of just FrodoKEM. I think draft-kampanakis-ml-kem-ikev2 gives us all necessary information how to use ML-KEM in IKEv2. In my opinion, an analogue draft describing the use of FrodoKEM in IKEv2 including assignment of IDs would be very helpful. I do not see the need to describe combinations of KEMs. If we do this, we will soon have large number of drafts describing every possible combination of KEMs.

Feedback on 23 May 2024

Yes, I am happy to remove ML-KEM in this draft, if other experts also think that the combination of ECDH+ ML-KEM+FrodoKEM is not necessary to be described here.

IKEv2 with FrodoKEM

Further Actions

- To add the details about fragmentation of PK and CT
- To align with ISO for acquiring its PQC KEM standardization progress?
- By IPSECME, PQUIP or CFRG?

Invitations

- Welcome to give your kind Suggestions and comments
- If you are interested in this work, welcome to let us know
- Wang.guilin@Huawei.com

Thanks!