Post-quantum Hybrid Key Exchange in the IKEv2 with FrodoKEM

IETF 121, IPSECME

Guilin Wang

Wang.guilin@Huawei.com

IKEv2 with FrodoKEM

❑ Information of our daft

- **Title**: Post-quantum Hybrid Key Exchange in the IKEv2 with FrodoKEM (draft-wang-hybrid-kem-ikev2-frodo-02)
- **Author**: Guilin Wang
- **Dates submitted**: v02 on 2024-10-18
- 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

❑ This Update

- V02: Changed the title, abstract and content to focus on using FrodoKEM, by following the comments from Leonie Bruckert on 15 May 2024.
- this talk: also show some experiments on using FrodoKEM.

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: Likely to be formally standardized around the end of 2025.

> [**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,

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

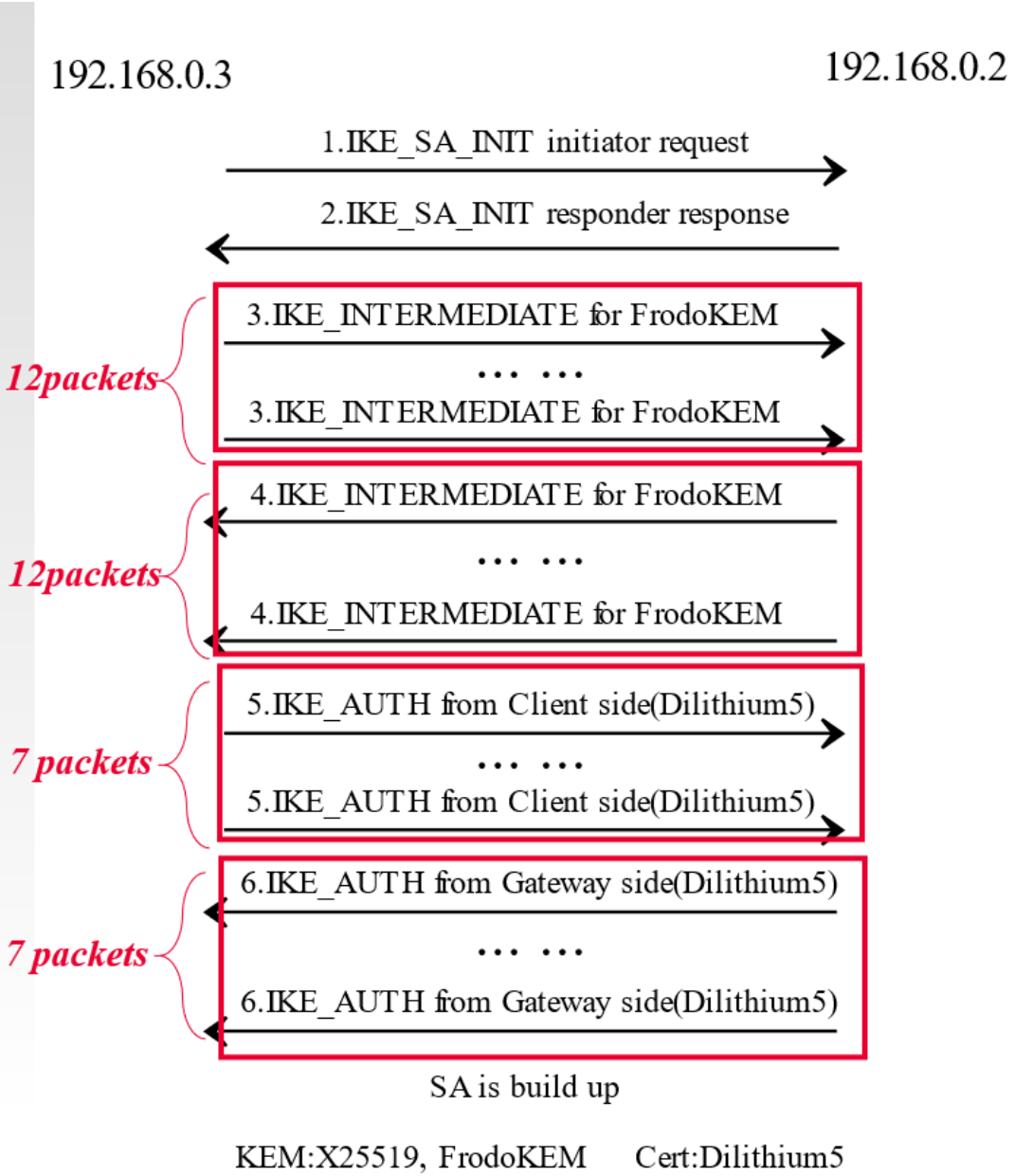
IKEv2 with FrodoKEM: An example

```
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: Experiment



Three Parameter Sets:

- Control group (X25519 + Dilithium5) : **16 packets**
- X25519_Kyber + Dilithium5: **18 packets**
- X25519_FrodoKEM(AES)+Dilithium5: **40 packets**

(shown left)

Experiment Environment:

- Open source software `strongswan` and the PQC version `pq-strongswan`.
- https://github.com/strongX509/docker/tree/master/pq-strongswan
- Measure the delay of the IKEv2 interaction between the client and gateway.

- Bandwidth: 80 Bps
- RTT: direct connected (nearly none)
- Packets loss: 0%, 1%, 2%, or 5%

IKEv2 with FrodoKEM: Experiment

Packet loss	0%	1%	2%	5%
X25519+Dilithium5	[26,26,26]	[26,228,4042]	[30,596,4053]	[26,762,4050]
X25519_Kyber+Dilithium5	[28,28,28]	[31,117,1263]	[98,622,4029]	[35,543,8052]
X25519_FrodoKEM+Dilithium5	[54,54,54]	[59,982,4895]	[68,1652,4689]	[4051,7451,12053]

Table. Time delay (smallest, average, largest) (ms) of different settings

Purpose: To measure the delay of the IKEv2 interaction between the client and gateway.

Our Testing Results:

- 30 times of experiments have been for each parameter set.
- When no packet loss, the IKEv2 delay between 3 set parameters is less than twice.
- When packet loss higher, the IKEv2 delay gets much higher, due to IKEv2 re-transmission mechanism: **wait for 4 seconds to re-transmit.**

IKEv2 with FrodoKEM

Further Actions

- More experiments
- 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!