Post-quantum Hybrid Key Exchange in the IKEv2 with FrodoKEM

IPSECME, IETF 122@Bangkok

Guilin Wang, Leonie Bruckert, and Valery Smyslov

IKEv2 with FrodoKEM

❑ Information of our daft

- **Title**: **Post-quantum Hybrid Key Exchange in the IKEv2 with FrodoKEM**
- draft-wang-ipsecme-hybrid-kem-ikev2-frodo-00 (replaced draft-wang-hybrid-kem-ikev2-frodo-02)
- **Date submitted**: 2025-3-03
- https://www.ietf.org/archive/id/draft-wang-ipsecme-hybrid-kem-ikev2-frodo-00.html

❑ 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

- Leonie and Valery joined the draft
- FrodoKEM referene updated, as suggeted by John Mattsson
- One reference added for the insecurity of SIDH
- Re-wrote Section 1 – Introduction, and corrected typos

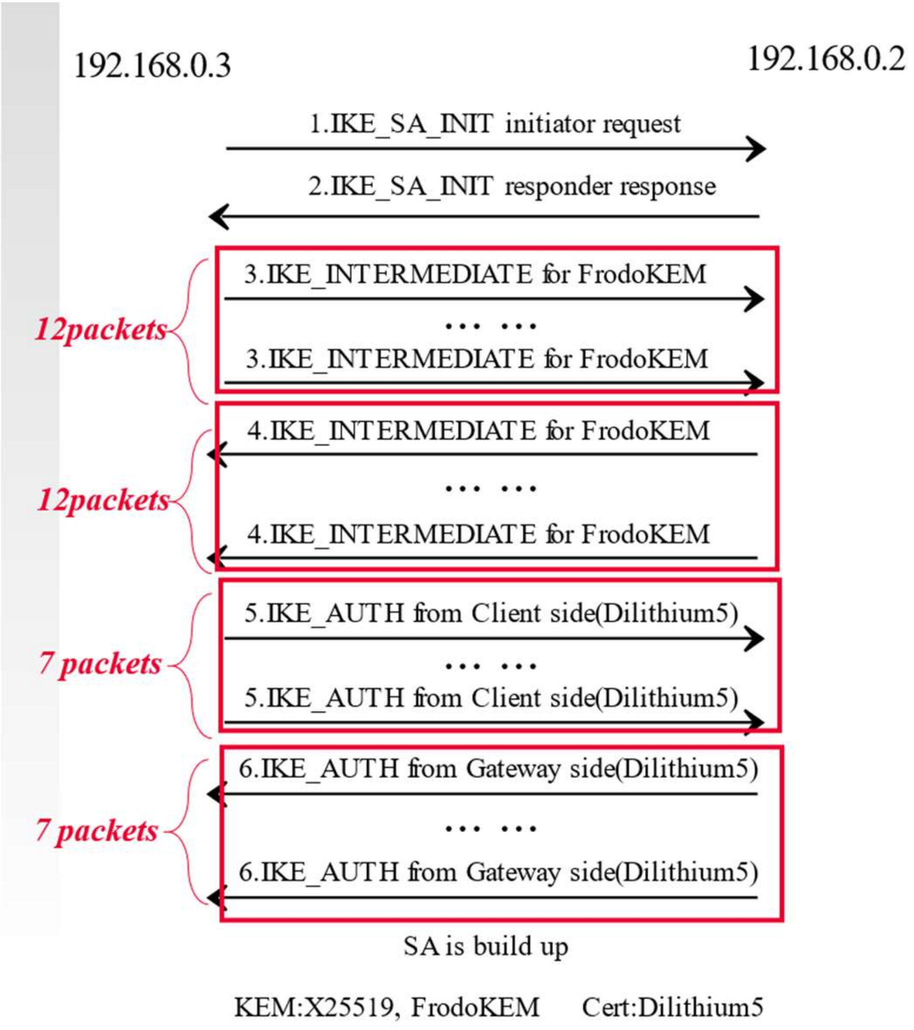
IKEv2 with FrodoKEM

❑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: Experiment



192.168.0.3

192.168.0.2

1.IKE_SA_INIT initiator request

2.IKE_SA_INIT responder response

12packets

3.IKE_INTERMEDIATE for FrodoKEM

… …

3.IKE_INTERMEDIATE for FrodoKEM

12packets

4.IKE_INTERMEDIATE for FrodoKEM

… …

4.IKE_INTERMEDIATE for FrodoKEM

7 packets

5.IKE_AUTH from Client side(Dilithium5)

… …

5.IKE_AUTH from Client side(Dilithium5)

7 packets

6.IKE_AUTH from Gateway side(Dilithium5)

… …

6.IKE_AUTH from Gateway side(Dilithium5)

SA is build up

KEM:X25519, FrodoKEM Cert:Dilithium5

Three Parameter Sets:

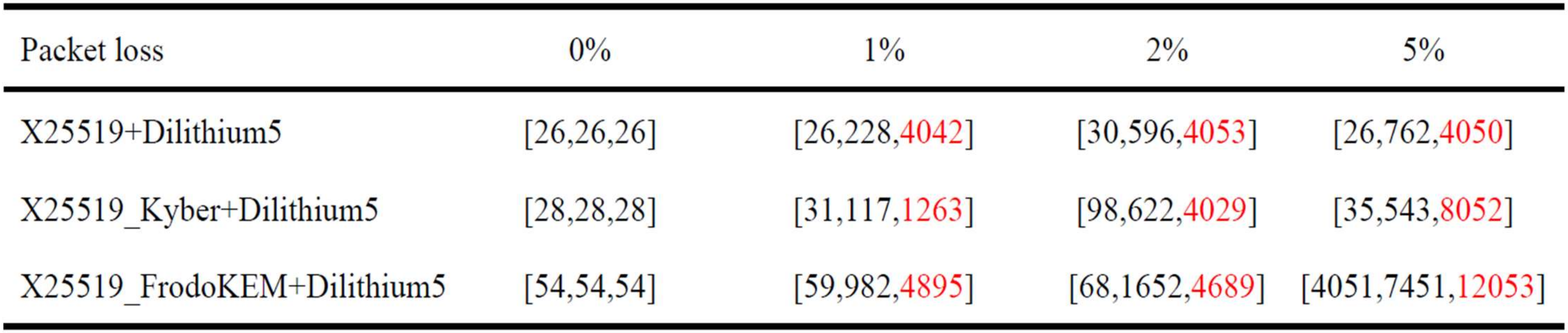
- Control group (X25519 + Dilithium5) : **16 packets**
- X25519_Kyber + Dilithium5: **18 packets**
- X25519_FrodoKEM(AES)+Dilithium5: **40 packets** **(shown left)**

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: Comments Received

Nov. 2024

John Mattsson: 10 November 2024 5:48 pm
There seems to be substantial interest in using FrodoKEM+ECC from European governments as it is seen as a conservative choice. My thought was that **ML-KEM+BIKE+ECC and ML-KEM+HQC+ECC seem like more conservative choices than FrodoKEM+ECC** ...

Patrick Longa: 14 November 2024 1:55 pm
- I see no fundamental reason to exclude FrodoKEM-AES. AES is *not* used as KDF in FrodoKEM, ... Similarly, any (future) Keccak/SHA-3 instructions are expected to give an additional speed boost to FrodoKEM-SHAKE.
- ... another possible dimension is the risk of structured versus unstructured schemes. See Chris Peikert's post on the NIST PQC mailing list.
- A comparison of 3-way hybrid schemes against 2-way hybrid schemes should definitely take into account other aspects such code complexity and compactness.

Paul Wouters: 18 November 2024 10:03 pm
I thought the world was moving towards ML-KEM and FrodoKEM? **It would be nice if we can wait for actual needs of something like Classic McEliece once we get there?**
...
I am open on looking at those, but would encourage us to not adopt documents for this **until it becomes clear there is an actual need.** With such a caveat, I think it is ok for some kind of mention in the charter.

Michael Richardson: 22 November 2024 12:25 am
I would like to be able to adopt without revising the charter, and I also think it's good to adopt documents much easier. (Even if we don't intend to finish them soon)

Jan. 2025

Paul Wouters: 11 January 2025 10:52 pm
I am interested in a pure mlkem and 25519mlkem hybrid. Possibly frodokem as alternative for mlkem.

John Mattsson: 22 January 2025 9:04 pm
I think IKEv2 should register code points for FrodoKEM and BIKE/HQC (depending on which one NIST standardizes). I think it is important with backups to ML-KEM. The importance of cryptographic agility has been emphasized by several US agencies.
...
FrodoKEM is unstructured but still lattice, BIKE/HQC is code-based but still structured. Many European governments are planning to use FrodoKEM as the main quantum-resistant algorithm for ephemeral-ephemeral key exchange. For an ESP association sending 100 GB of data, the overhead of FrodoKEM and BIKE/HQC is small.
...
I think CFRG should specify FrodoKEM, but I am also fine with continue using frodokem.org as a normative reference.

Watson Ladd: 23 January 2025 12:44 am
The relevant registry is expert review, so you can just do that.

IKEv2 with FrodoKEM: Comments Received

Scott Fluhrer: 23 January 2025 1:27 am

There exist standards for FrodoKEM now, so you could point to those documents (or does IANA insist they be IETF documents?)

Loganaden Velvindron: 23 January 2025 2:11 am

Indeed. Cryptographic agility is good. I've also seen this from wolfssl: https://www.wolfssl.com/coming-soon-frodokem-in-wolfcrypt/

Michael Osborne: 23 January 2025 3:37 am

You want to check this statement "Many European governments are planning to use FrodoKEM as the main quantum-resistant algorithm for ephemeral-ephemeral key exchange"

The Netherlands have already updated guidance such that ML-KEM is recommended and FrodoKEM is acceptable.
https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf
I understand BSI Germany and others will do the same shortly

John Mattsson: 23 January 2025 2:11 pm

I do not think IETF should normatively refer to paywalled ISO crypto standards, ...

I think the draft/RFC should be updated to the latest version on frodokem.org
https://frodokem.org/files/FrodoKEM_standard_proposal_20241205.pdf

John Mattsson: 23 January 2025 2:29 pm

ANSSI, BSI, and Swedish NCSA have all just recently added ML-KEM to their list of recommended algorithms, which I very much welcome, but I have not seen any indication that they would stop recommending FrodoKEM. My current understanding is that many European governments are planning to use FrodoKEM as the main quantum-resistant algorithm for ephemeral-ephemeral key exchange for their national security systems. Like the US more algorithms might be allowed for government systems that are not national security systems.

- https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_stephan-ehlen_bsi_post-quantum-policy-and-roadmap-of-the-bsi.pdf
- https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_jerome-plut_anssi_anssi-plan-for-post-quantum-transition.pdf
- https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf
- https://cyber.gouv.fr/sites/default/files/document/pqc-transition-in-france.pdf
- http://kth.diva-portal.org/smash/get/diva2:1902626/FULLTEXT01.pdf

John Mattsson: 23 January 2025 2:44 pm

We are not currently planning to use FrodoKEM, BIKE, HQC, but would like to a subset of them supported as backup algorithms for ephemeral encapsulation keys.

IKEv2 with FrodoKEM: Comments Received

Michael Osborne: 23 January 2025 4:25 pm

I may speak to a different cohort than you, but the shift that I notice is nuanced in “recommended” vs “allowed”. Not sure how much this matters – just wanted to tell you what I see.

John Mattsson: 23 January 2025 5:06 pm

Thanks, I have not noticed that change in nuance except from The Netherlands. Important to remember that there are many European countries and that they do not agree on everything. The best thing would be if representatives for the European countries could speak up so we don’t have to speculate. They are probably all on this list…

Paul Wouters: 24 January 2025 11:34 am

I did not myself yet look into the text as written. **But I think something generic like I wrote above should apply,** irrespective of the algorithms plugged in (ML-KEM+25519, FrodoKEM+25519, or even 25519+P256)

Feb. 2025

Valery Smyslov: 21 February 2025 8:54 pm

…

On the other hand, I hope that adoption call(s) for PQ KEMs are started soon (draft-kampanakis-ml-kem-ikev2, draft-wang-hybrid-kem-ikev2-frodo etc.)

Michael Richardson: 25 February 2025 3:29 am

For #1, we have:
draft-kampanakis-ml-kem-ikev2-09
and draft-wang-hybrid-kem-ikev2-frodo-02

I would prefer to have a single document: "Quantum-Safe Algorithms and Methods for IKEv2", which took all these document together.

I would call upon the chairs to use your perogative to create a design team on this topic, inviting the authors of all these documents to work together.

Short Summary:

- 20+ emails in 4 months from 9 experts
- 18 emails shown here
- Majority supportive to register code points for FrodoKEM, as main or back up KEM algorithm
- Good support from some EU authorities
- SEC AD: concern about “actual needs”
- One whole document for both ML-KEM and FrodoKEM, or separate?

IKEv2 with FrodoKEM

Further Actions

- Group Adoption?
- …

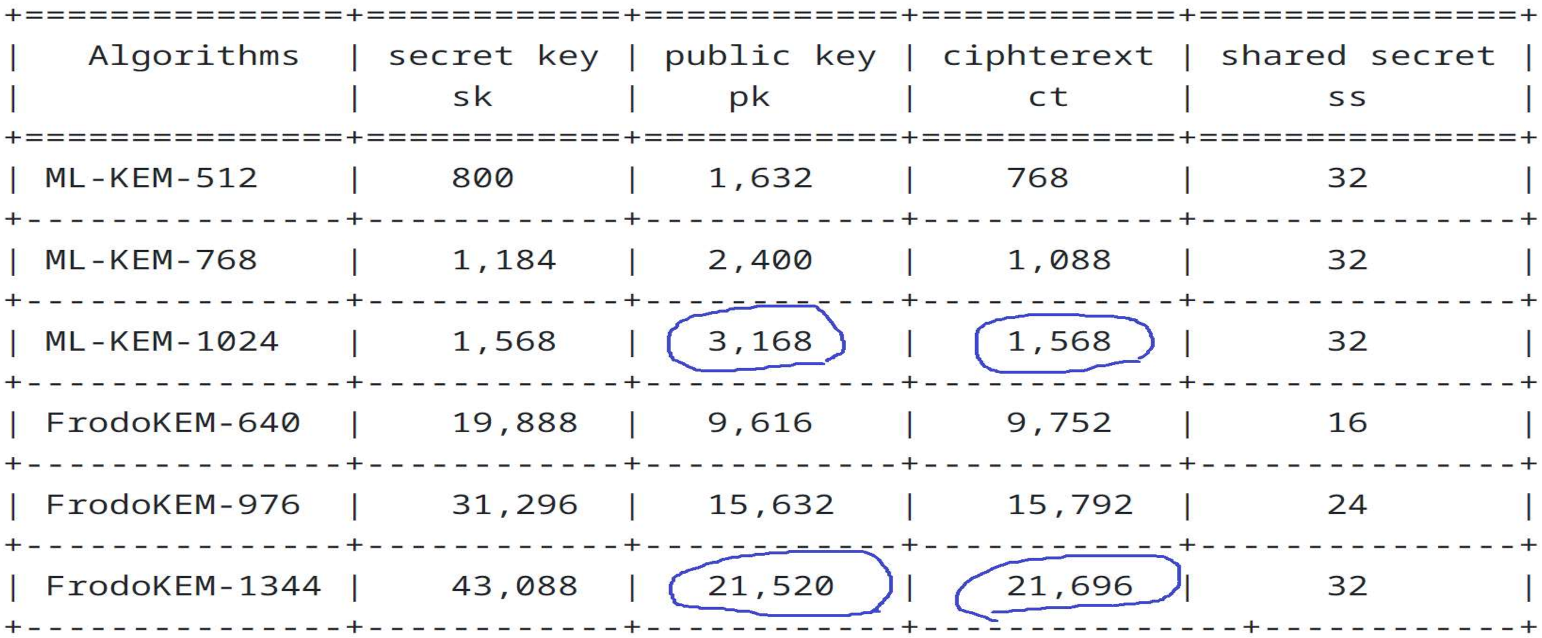
Welcome to give your comments

- Wang.guilin@Huawei.com
- Leonie.Bruckert@secunet.com
- svan@elvis.ru

Thanks!

IKEv2 with FrodoKEM: Challenges

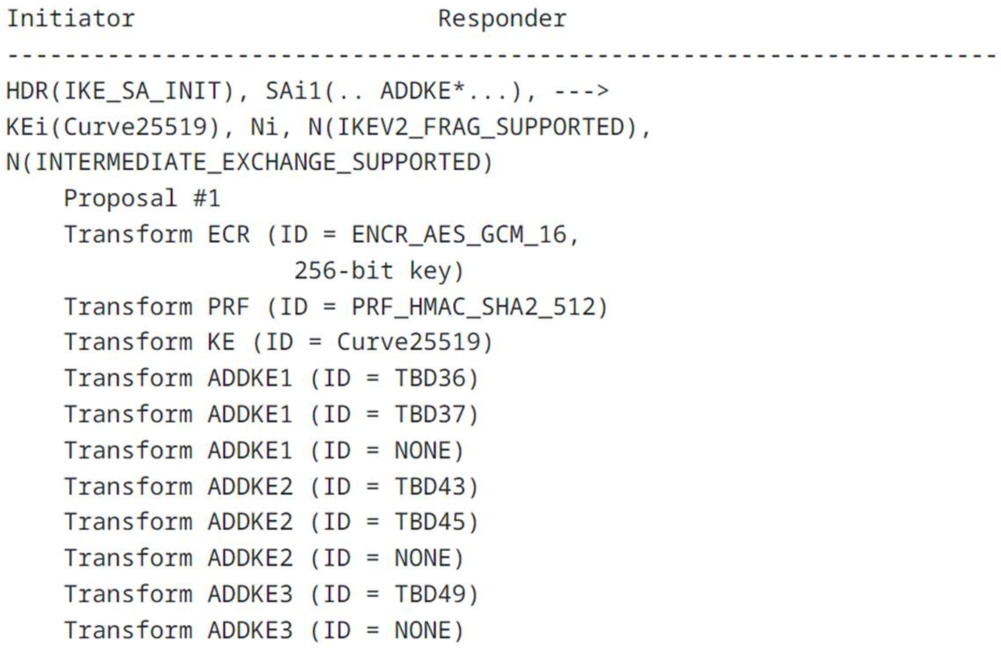
- **Communication**: The public key and ciphertext of FrodoKEM is about 10 times of ML-KEM
- Luckily, the IKE Intermediate Exchange supports large message exchange (but less than 2^{16} - 1 = 65,535 Bytes) (RFC 9242, RFC 7383)
- Also, need 8 or 12 OIDs: Most likely, ISO shall go for 8 parameter sets



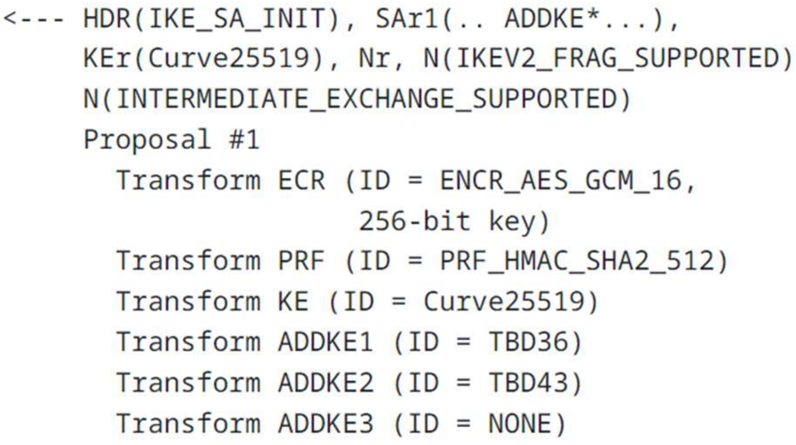
Algorithms	secret key sk	public key pk	ciphterext ct	shared secret ss
ML-KEM-512	800	1,632	768	32
ML-KEM-768	1,184	2,400	1,088	32
ML-KEM-1024	1,568	3,168	1,568	32
FrodoKEM-640	19,888	9,616	9,752	16
FrodoKEM-976	31,296	15,632	15,792	24
FrodoKEM-1344	43,088	21,520	21,696	32

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

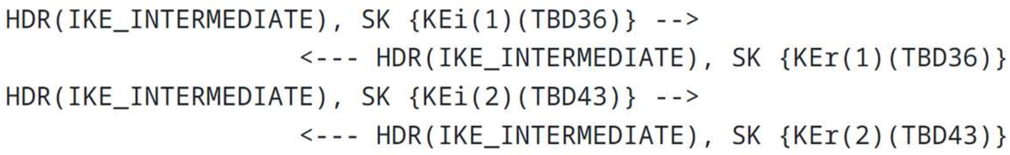
IKEv2 with FrodoKEM: An example



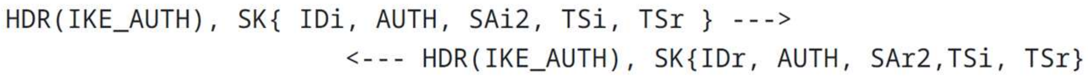
```
Initiator                          Responder
-------------------------------------------------------------------
HDR(IKE_SA_INIT), SAi1(.. ADDKE*...), --->
KEi(Curve25519), Ni, N(IKEV2_FRAG_SUPPORTED),
N(INTERMEDIATE_EXCHANGE_SUPPORTED)
    Proposal #1
    Transform ECR (ID = ENCR_AES_GCM_16,
                    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}
```