Comparison of hybrid KEM drafts across WGs

ENTRUST

Comparison

Draft	Purpose	Combiner
cfrg-kem-combiners	Abstract construction. Secure in “worst case”.	KDF(ct1, ss1, ct2, ss2) * ct and ss must be length-encoded if not constant length.
tls-hybrid-design	Ephemeral-ephemeral key exchange embedded within the TLS handshake.	ss1 || ss2 --> HKDF-EXTRACT transcript(including ct1, ct2) --> HKDF-EXTRACT
crfg-hpke-xyber768d00	Add X25519Kyber768 to HPKE (RFC 9180).	ss1 || ss2
lamps-composite-kem	Public keys for KEM X.509 certificates. For use anywhere that needs X.509 encryption certs. CMS, S/MIME – typically one-shot KEM for CEK key wrapping.	cfrg-kem-combiners with KMAC{128,256}
openpgp-pqc	OpenPGP Long-lived public keys. One-shot KEM for CEK key wrapping.	cfrg-kem-combiners with KMAC256
jose-hybrid-encrypt	JOSE / COSE Long-lived public keys. One-shot KEM for CEK key wrapping.	cfrg-kem-combiners with KMAC256

Hybrid Algorithm Alignment

* This is close to aligned,
but not perfect. … missing P521??

X	ML-KEM-512	ML-KEM-768	ML-KEM-1024
RSA	lamps-composite-kem	lamps-composite-kem	
ECDH-P256	lamps-composite-kem jose-hybrid-encrypt	tls-hybrid-design lamps-composite-kem openpgp-pqc	
ECDH-Brainpool-P256	lamps-composite-kem	lamps-composite-kem openpgp-pqc	
X25519	lamps-composite-kem jose-hybrid-encrypt	tls-hybrid-design crfg-hpke-xyber768d00 lamps-composite-kem openpgp-pqc jose-hybrid-encrypt	
ECDH-P384		jose-hybrid-encrypt *	lamps-composite-kem openpgp-pqc
ECDH-Brainpool-P384			lamps-composite-kem openpgp-pqc
X448			lamps-composite-kem openpgp-pqc

Aside: SP 800-56Cr2 shared secret combiners

"this Recommendation permits the use of a "hybrid" shared secret of the form Z' = Z || T"

- *HASH(), HMAC-hash()* or *KMAC#()*
- *counter* || *Z* || *FixedInfo*
  - counter starts at 0x00000000; if using HASH() on large input then you need to iterate and increment *counter*.

- draft-ounsworth-cfrg-kem-combiners is the direct instantiation of this (ie trivial FIPS-compliance).
- tls-hybrid-design and cfrg-hpke-xyber should be compliant with some explaining.

ENTRUST

draft-ounsworth-cfrg-kem-combiners

Authors: Mike Ounsworth, Aron Wussler, Stavros Kousidis

Purpose:

Defines an abstract KDF construction, compatible with NIST SP 800-56Cr2, suitable for combining two or more KEMs such that the overall combined KEM will be IND-CCA2 so long as at least one of the component KEMs is.

Construction:

```
ss = KDF(counter || k_1 || ... || k_n || fixedInfo, outputBits)
  Where:
k_i = (ct_i || ss_i)     -- if constant-length
  OR
k_i = (ct_i || rlen(ct_i) || ss_i || rlen(ss_i) )
```

Instantiations:

KDF = KMAC128, KMAC256, SHA3-256, or SHA3-512.

Does not provide concrete instantiations of component KEMs.

ENTRUST

draft-ietf-tls-hybrid-design

Authors: Douglas Stebila, Scott Fluhrer, Shay Gueron

Purpose:

“This document focuses on hybrid ephemeral key exchange in TLS 1.3”

Construction:

```
ss1 || ss2 --> HKDF-EXTRACT
transcript(including ct1, ct2) --> HKDF-EXTRACT
```

Also compatible with NIST SP 800-56Cr2.

This is very close to being an instantiation of cfrg-kem-combiners; includes ss’s and ct’s in “cascading” mode, compared to cfrg-kem-combiner’s “concatenated” mode.

Forgoes length-encoding because X25519, SecP256r1 and Kyber are fixed-length.

Instantiations:

X25519Kyber768Draft00, SecP256r1Kyber768Draft00

ENTRUST

draft-draft-westerbaan-cfrg-hpke-xyber768d00

Authors: Bas Westerbaan, Chris Wood

Purpose:

> *“This memo defines X25519Kyber768Draft00, a hybrid post-quantum KEM, for HPKE (RFC9180).*
> *In short, X25519Kyber768Draft00 is the parallel combination of DHKEM(X25519, HKDF-SHA256) [RFC9180] [RFC7748] and Kyber768Draft00 [KYBER].”*

Construction:

```
ss1 || ss2
```

OK to not include ct’s because both DHKEM(X25519) and Kyber768Draft00 already mix in ct’s.

OK to not include KDF at this layer because HPKE (RFC9180) will subsequently pass the ss through HKDF … so it still compliant with NIST SP 800-56Cr2.

Instantiations:

X25519Kyber768Draft00

ENTRUST

draft-draft-westerbaan-cfrg-hpke-xyber768d00

Authors: Bas Westerbaa

Purpose:

"This memo defines X *d post-quantum KEM, for HPKE (RFC9180).*
In short, X25519Kybe *ination of DHKEM(X25519, HKDF-SHA256) [RFC9180] [RFC7748] a* *768Draft00 [KYBER]."*

Note:
No longer true if we're talking about ML-KEM-ipd!

So does that mean the protocol now needs to commit the ciphertext?

Construction:

```
ss1 || ss2
```

OK to not include ct's because both DHKEM(X25519) and Kyber768Draft00 already mix in ct's.

OK to not include KDF at this layer because HPKE (RFC9180) will subsequently pass the ss through HKDF … so it still compliant with NIST SP 800-56Cr2.

Instantiations:

X25519Kyber768Draft00

ENTRUST

draft-ietf-lamps-composite-kem

Authors: Mike Ounsworth, John Gray, Max Pala, Jan Klaußner, Scott Fluhrer

Purpose:

> *“This document defines Post-Quantum / Traditional composite Key Encapsulation Mechanism (KEM) algorithms suitable for use within X.509 and PKIX and CMS protocols.”*

Construction:

cfrg-kem-combiners with KMAC128 or KMAC256, matching the security level of component KEMs.

Instantiations:

Given the wide range of applications of X.509 encryption certificates, a broader set of instantiations is provided (see next slide).

ENTRUST

draft-ietf-lamps-composite-kem Registered Algorithms

id-MLKEM512-RSA2048-KMAC128

id-MLKEM512-ECDH-P256-KMAC128

id-MLKEM512-ECDH-brainpoolP256r1-KMAC128

id-MLKEM512-X25519-KMAC128

id-MLKEM768-RSA3072-KMAC256

id-MLKEM768-ECDH-P256-KMAC256

id-MLKEM768-ECDH-brainpoolP256r1-KMAC256

id-MLKEM768-X25519-KMAC256

id-MLKEM1024-ECDH-P384-KMAC256

id-MLKEM1024-ECDH-brainpoolP384r1-KMAC256

id-MLKEM1024-X448-KMAC256

It's the permutations of:

ML-KEM
X
{ RSA,
ECDH-SecP,
ECDH-brainpool,
ECDH-Edwards }

ENTRUST

draft-wussler-openpgp-pqc

Authors: Stavros Kousidis, Falko Strenzke, Aron Wussler

Purpose:

Provide OpenPGP with composite public-key encryption based on ML-KEM in combination with elliptic curve cryptography because OpenPGP has already deprecated RSA.

Construction:

cfrg-kem-combiners with KMAC256.

Instantiations:

ML-KEM-768_x25519Kem, ML-KEM-1024_x448Kem,
ML-KEM-768_ecdhKemNISTP-256, ML-KEM-1024_ecdhKemNISTP-384,
ML-KEM-768_ecdhKemBrainpoolP256r1, ML-KEM-1024_ecdhKemBrainpoolP384r1

ENTRUST

draft-ra-jose-hybrid-encrypt

Authors: Tirumaleswar Reddy, Aritra Banerjee

Purpose:

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

Note: this is a competing proposal to getting it “for free” from HPKE-xyber.

Construction:

cfrg-kem-combiners with KMAC256.

Instantiations:

x25519-ES_kyber512, secp384r1-ES_kyber768, x25519-ES_kyber768, secp256r1-ES_kyber512

ENTRUST

Summary

Combiner construction

- `cfrg-kem-combiners` is intended to be “overkill”.
  - `lamps-composite-kem`, `openpgp-pqc`, `jose-hybrid-encrypt` directly chain to cfrg-kem-combiners.
  - Open question: can `cfrg-kem-combiners` safely be further relaxed?
- `tls-hybrid-design` and `crfg-hpke-xyber768d00` relax the combiner construction from cfrg-kem-combiners because their respective protocols (TLS and HPKE) already include ct’s and an HKDF.
- These constructions are all cryptographically equivalent.

Supported algorithm combinations

- Algs are more aligned than it may appear at first glance; we are very close to:

`lamps-composite-kem` ⊃ `openpgp-pqc` ⊃ `jose-hybrid-encrypt` ⊃ `tls-hybrid-design` ⊃ `crfg-hpke-xyber768d00`

(where ⊃ is “superset”)

ENTRUST

Summary

Instantiating cfrg-kem-combiners

`crfg-hpke-xyber768d00` provides a really nice template for how to “instantiate” `crfg-kem-combiners`:

3. Construction

   …

   ```
   return concat(ss1, ss2)
   ```

4. Security Considerations

   Identify and justify the difference from cfrg-kem-combiners.

   “In the present case, DHKEM(X25519, -) and Kyber768Draft00 already mix in the respective cipher texts into their shared secrets.

   Furthermore, in HPKE, the shared secret is never used directly, but passed through HKDF (via KeySchedule), and thus we can forgo the call to HKDF as well.”

ENTRUST