draft-ietf-lamps-pq-composite-kem

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

“The elephant in the room”

Summary of CRFG Hybrid KEMs status

For those not following CFRG, summary:

- On 2024-01-31 the CFRG chairs started a call for adoption for the entire research area of Hybrid KEM Combiners.
- The call for adoption was left open for 5 weeks.
  - The thread received ~ 150 responses.
- Consensus: Yes, the topic should be adopted. CFRG chairs to form a design team.
- In true IETF fashion, we all agree that a small number of well-constructed hybrid KEMs should be produced by CFRG and used by all IETF WGs, but long heated disagreements about which ones.

Changes in version -03

- Changed the title to reflect that it is specific to ML-KEM.
  - Title is now “**Composite ML-KEM for Use in the Internet X.509 Public Key Infrastructure and CMS**”
- Added Max Pala, Jan Klaussner, and Scott Fluhrer as authors.
- Added text to Introduction to justify where and why this mechanism would be used.
- Added section "Use in CMS".
  - We know that convention is to define algorithms and CMS usage in separate documents, so this text was written so that it can be split out to a separate document if we want.
- Switched all KDFs for both the combiner and the CMS KEMRI to use id-kmac128 or id-kmac256 from I-D.ietf-lamps-cms-sha3-hash. This aligns with draft-ietf-lamps-cms-kyber-03.

Still to do

- Samples
  - The hackathon is starting to provide usable samples for both composite KEM certificates, and usage for payload encryption with CMS.
- Synchronize with the outcome of the CFRG effort, and other similarly-behaving hybrid KEMs in HPKE, JOSE / COSE, OpenPGP – protocols that, like PKIX, expect long-lived non-ephemeral KEM keys.
- Some open discussion points…

Discussion point #1 Alignment with CFRG and other hybrid KEMs in other WGs.

“The elephant in the room”.

Ultimately, yes, this LAMPS work cannot move faster than the security analysis in CFRG, and hybrid KEM drafts in parallel WGs.

This draft is likely to change to align with other work.

Discussion point #2 Also provide HMAC-SHA2 combiners and KEMRI instantiations?

- This was brought up at PQUIP 118.
- The point was made that, yes, ML-KEM requires SHA3 internally, but the layer of software doing the combiner may not have access to a SHA3 implementation.
- However, it is not entirely clear that you can replace KMAC with HMAC-SHA2 without changing the security properties of the dual-input combiner.

Discussion point #3 UKM

Russ said:

“Do any of your composite KEM algorithms require a UKM? I can imagine a way to use DH and ECDH that require a UKM”

I think the exact construction of the combiner, and whether anything, such as receiver public keys, need to be treated as a “UKM” is one of the issues to be studied in CFRG.

Summary

- Stable … for now.
- Hackathon artifacts are growing.
- Heavily pending outcome of CFRG action.