DRAFT-OUNSWORTH-CFRG-KEM-COMBINERS-01

IETF 116 – CFRG

Mike Ounsworth, Aron Wussler, Stavros Kousidis

ENTRUST

PQ HYBRID KEMS ARE EVERYWHERE

(and if not, they’re gonna be)

- draft-ietf-tls-hybrid-design-05
- draft-ounsworth-pq-composite-kem-00
- draft-wussler-openpgp-pqc-01
- (draft-tjhai-ipsecme-hybrid-qske-ikev2-00)
- … there are sure to be more.

- CFRG should standardize the safe way to combine two shared secrets.

draft-ounsworth-cfrg-kem-combiners-01

ENTRUST

GOALS OF THIS DRAFT

We are hoping for a document, similar to HPKE 9180, **that is secure in the most general case**, which I believe is CMS / S/MIME where people are free to do a key encapsulation against static long-term keys using arbitrarily bad KEM algorithms (such as RSA-KEM RFC5990).

What about simpler combiners?

draft-ietf-tls-hybrid-design and draft-wussler-openpgp-pqc want to trade stronger assumptions about input KEMs for a simpler combiner.

Paul Hoffman suggested that this draft collect, in an appendix, these special-purpose combiners and the assumptions that make them sound in their context?

draft-ounsworth-cfrg-kem-combiners-01

ENTRUST

OUR APPROACH

We need a “cfrg-kem-combiners” I-D to exist.

We don’t feel qualified to write one.

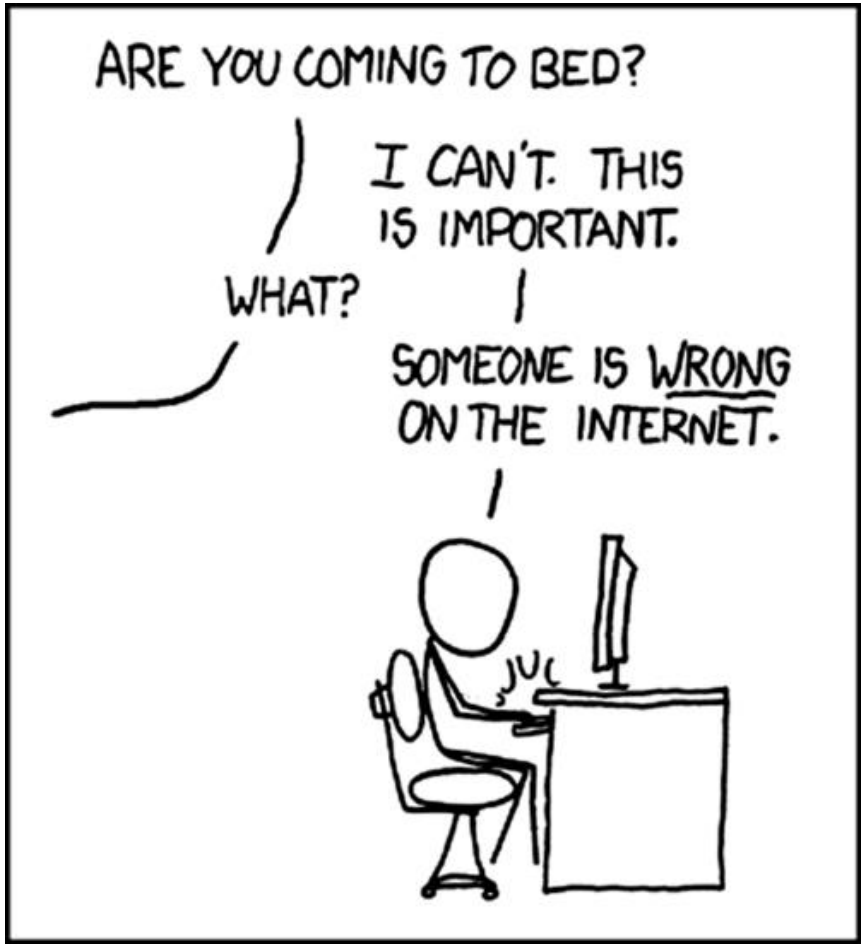
Nobody else seems to be writing one.

So…

Step 1: write a draft.

Step 2: wait for people to yell at us about why it’s wrong.

Step 3: profit.



draft-ounsworth-cfrg-kem-combiners-01

ENTRUST

THE PROPOSED KEM COMBINER

SS = KDF(counter || k_1 || ... || k_n || fixedInfo, outputBits)

Where

- **k_i = H(ss_i || ct_i)** protects against both chosen ciphertext attacks, and collision attacks in the underlying hash function of **KDF.**
- KDF = SHA3-256 and H = SHA3-256, with hashSize = 256 bit.
  KDF = KMAC128 and H = SHA3-256, with hashSize = 128 bit.
  KDF = SHA3-512 and H = SHA3-512, with hashSize = 512 bit.
  KDF = KMAC256 and H = SHA3-512, with hashSize = 256 bit.
- **fixedInfo** is to be filled with any available context-binding information from the protocol.

This is compliant with NIST SP 800-56Cr2.

That's it. Please yell at us on the mailing list about why this is terrible.

WARNING: if you yell usefully enough, we'll make you a co-author.

draft-ounsworth-cfrg-kem-combiners-01

ENTRUST

Adoption?

draft-ounsworth-cfrg-kem-combiners-01

ENTRUST