

KEM Combiners

draft-ounsworth-cfrg-kem-combiners-04

Mike Ounsworth

Aron Wussler

Stavros Kousidis

IETF 117

2023-07-25

Changes since -03

- Removed intermediate hashing in favor of length encoding (for variable length inputs)
- Adapted the construction to streaming
- Preferred KMAC-based constructions
- “multi-PRF” -> “split-key PRF”, more formally defined

Open issues from the list

- #10: Clarify reliance on RO assumption for Keccak
- #14: Add recommended default value for KMAC key
- #15: Consider HMAC-based constructions

Updated construction

```
KDF(counter ||  
      ct_1 || rlen(ct_1) || ss_1 || rlen(ss_1) ||  
      ct_2 || rlen(ct_2) || ss_2 || rlen(ss_2) ||  
      ...  
      fixedInfo,  
      outputBits)
```