Hybrid KEMs

draft-irtf-cfrg-hybrid-kems-07
draft-irtf-cfrg-concrete-hybrid-kems-02

IETF 124 - Montreal

Agenda

The Brief

Changes since IETF 123 and the September interim

Update on security analysis

Questions for feedback

The Brief

CFRG email 2024-07-10

Also:

- Provide guidance that lets non-cryptographers make safe hybrid KEMs
- Provide some targets for the ecosystem to converge on
- Alignment with LAMPS, OpenPGP, X-Wing

(A) Identify which KEM security properties are IETF-relevant, and provide a terse overview of those security properties (eg. IND-CCA, LEAK-BIND-K-PK, HON-BIND-K-CT, etc), as well as security properties unique to hybrid KEMs (component key material reuse between hybrid and non-hybrid uses or between multiple hybrids, one component is malicious while the other is honest, etc) with reference to literature, and put into context with real-world attacks. From that, give guidance on a sensible baseline.

(B) Provide a terse overview of well-reviewed techniques that are options to safely produce the concrete combinations in (C), and which security properties are achieved given those of the constituents.

(C) Provide an initial number of explicit PQ/T hybrid KEMs using techniques from (B) that reach the baseline set in (A), and should include:

(I) a hybrid of P-256 and ML-KEM-768,
(II) a hybrid of X25519 and ML-KEM-768, and,
(III) a hybrid of P-384 and ML-KEM-1024.

These hybrids should be accompanied by pseudocode and test vectors.

draft-irtf-cfrg-hybrid-kems

- Now four (4) generic frameworks:
  - UK (was ‘GHP’), CG (was ‘QSF’), UG (new!), CK (new!)
  - Removed ‘PRE’
- Tidied up how to write all these out
- Default keygen for all frameworks is seed-based, while specific concrete instantiations MAY deviate (with language on the security implications)
- Added IANA registry for domain separation labels
- Fleshed out binding property proofs for all frameworks
- IND-CCA proofs for UG and and CK exist, being prepared for publication

Current set of constructions: Four variants

KDF(concat(...))	PQ ≥ 0 (broken = no assumption)	PQ ≥ C2PRI (broken = still assume C2PRI)
T=Group	ss_PQ, ss_T, **ct_PQ,** ct_T, **ek_PQ,** ek_T, label (ct_T, ek_T = **group elements**)	ss_PQ, ss_T, ~~**ct_PQ,**~~ ct_T, ~~**ek_PQ,**~~ ek_T, label (ct_T, ek_T = **group elements**)
T=KEM	ss_PQ, ss_T, **ct_PQ,** ct_T, **ek_PQ,** ek_T, label (ct_T, ek_T = **KEM ciphertext, enc. key**)	ss_PQ, ss_T, ~~**ct_PQ,**~~ ct_T, ~~**ek_PQ,**~~ ek_T, label (ct_T, ek_T = **KEM ciphertext, enc. key**)

New: IANA registry “Hybrid KEM Labels”

Label	Framework	PQ	T	KDF	PRG	Nseed	Nss	Reference
“\.//^\”	CG	ML-KEM-768	X25519	SHA3-256	SHAKE256	32	32	[CONCRETE]
“MLKEM…”	CG	ML-KEM-768	P-256	SHA3-256	SHAKE256	32	32	[CONCRETE]

Labels are supposed to uniquely identify hybrid KEM instantiations

The usual I*TF mechanism for uniqueness is an IANA registry

First Come First Served policy

draft-irtf-cfrg-concrete-hybrid-kems

- Scheme names aligned with generic doc
- Labels and IANA registrations for them
- Fix P-256/P-384 scalar moduli
- Rejection sampling instead of wide reduction for NIST curve `RandomScalar`
- Nail down requirements for HKDF usage
- Corresponding updates to reference implementation and test vectors

Labels, again

- PR#28 made labels different from names because the names kept changing and people wanted something stable
- The choice of non-name labels caused some consternation
- We ran a quick poll which showed support for semantic labels again
- A PR implementing this change this has been merged:
  - `CG(ML-KEM-768 + X25519) = "\.//^\"` (unchanged)
  - `CG(ML-KEM-768 + P-256) = "MLKEM768-P256"`
  - `CG(ML-KEM-1024 + P-384) = "MLKEM1024-P384"`
- LAMPS composite KEMs has updated but needs to be pushed to datatracker
- Confirmed interop between the reference implementation and Mike Ounsworth's LAMPS test stack

Next steps

At this point, we do not intend an further changes to the constructions

- Need to rev `draft-irtf-cfrg-hybrid-kems` once proofs for UG and CK are published
- Then on to the crypto review panel and RGLC

Hybrid KEMs

draft-irtf-cfrg-hybrid-kems-07
draft-irtf-cfrg-concrete-hybrid-kems-02

IETF 124 - Montreal