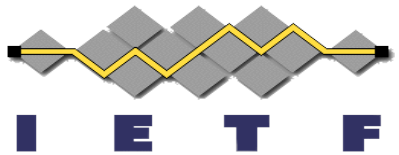
PQ/T Hybrid KEM: HPKE with JOSE/COSE

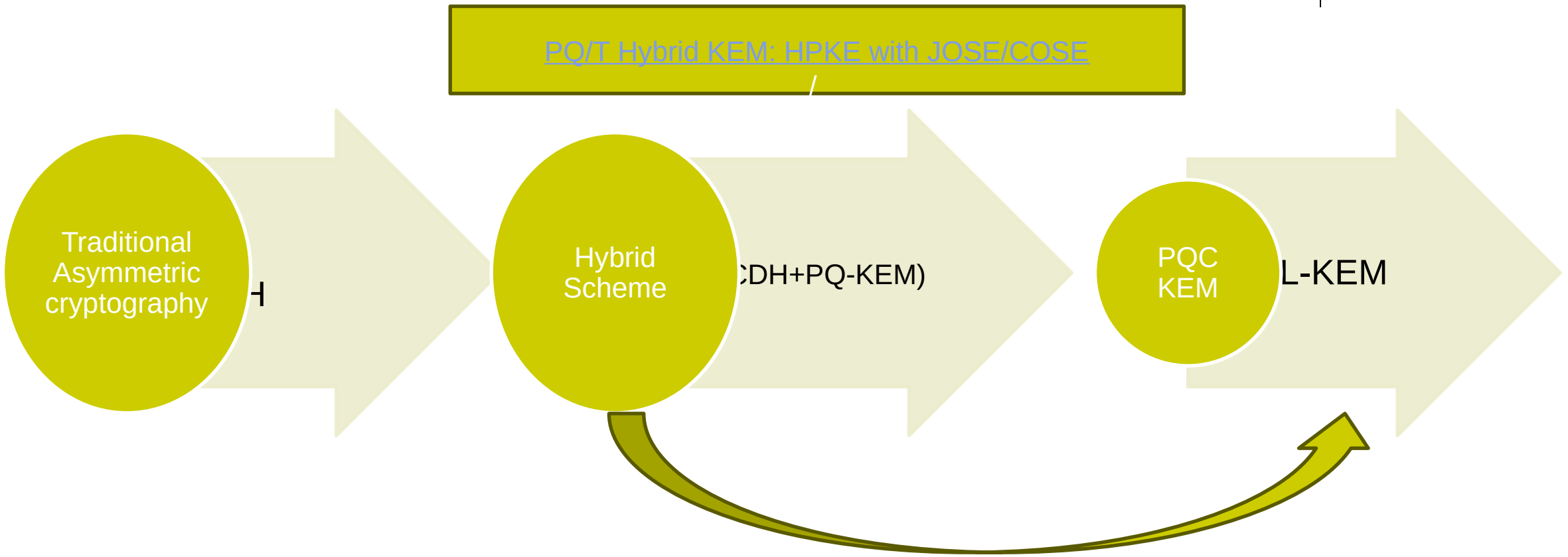


draft-reddy-cose-jose-pqc-hybrid-hpke

Tirumaleswar Reddy, **Hannes Tschofenig**

IETF 121, Dublin

Transition path



PQ/T Hybrid KEM

- *PQ/T Hybrid Key Encapsulation Mechanism (KEM)*: A multi-algorithm KEM made up of two or more component algorithms where at least one is a post-quantum algorithm and at least one is a traditional algorithm.
  - The term is defined in https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/
  - Protocols like TLS (ietf-tls-hybrid-design) and IKEv2 (RFC9242) already use Hybrid Key Exchange schemes.

PQ-KEM Encapsulation

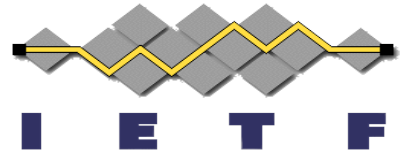
- https://datatracker.ietf.org/doc/draft-connolly-cfrg-xwing-kem/ defines Hybrid PQ/T KEM.
- It uses both Traditional (X25519) and PQC Algorithm (ML-KEM768) to derive the final shared secret

HPKE Mode

- PQ/T Hybrid KEM in HPKE is not an authenticated KEM.
- Authenticated KEM is only possible when both parties contribute a PQC KEM public key and a traditional public key to the overall session key.
- The HPKE Base mode can only be supported with the PQ/T Hybrid KEM.

- Updated draft to address comments, align with the final FIPS 203 (MLKEM) and COSE/JOSE HPKE drafts.

JOSE Algorithm Registry



Name: HPKE-X25519MLKEM768-SHA256-AES256GCM

Algorithm Usage Location(s): "alg“

Description: Cipher suite for JOSE-HPKE in Base Mode that uses the X25519MLKEM768 Hybrid KEM, the HKDF-SHA256 KDF, and the AES-256-GCM AEAD.

Next Steps

- Consider for WG adoption
- Comments and suggestions are welcome