Post-Quantum and Hybrid enhancements for EAP-AKA’

https://datatracker.ietf.org/doc/draft-ietf-emu-hybrid-pqc-eapaka/
https://datatracker.ietf.org/doc/draft-ietf-emu-pqc-eapaka/

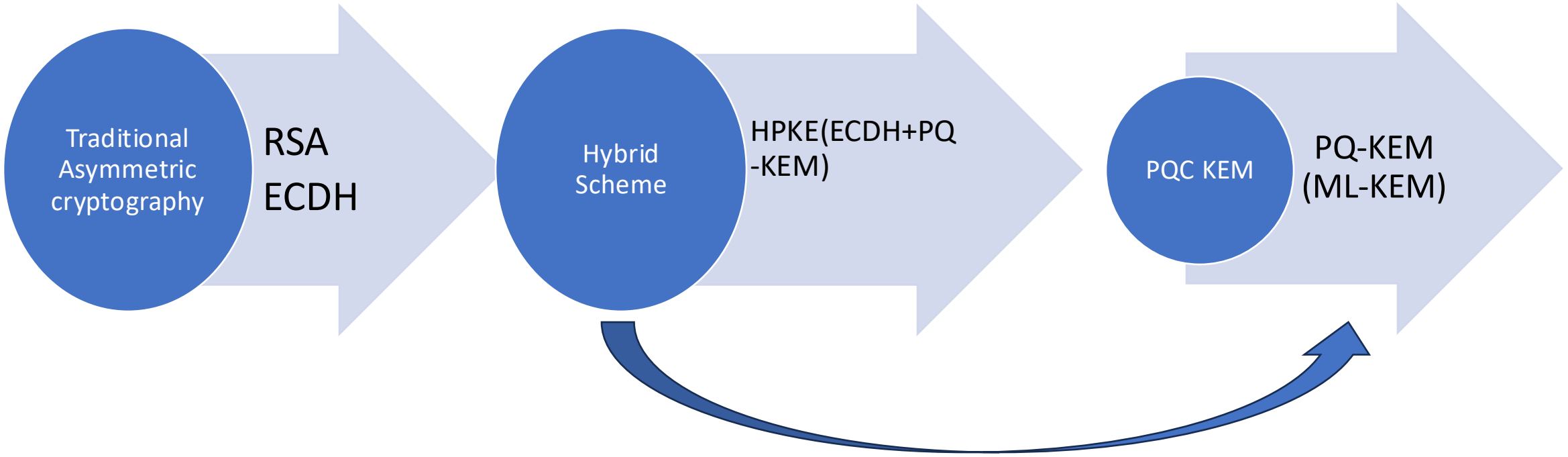
IETF 123 Madrid

Aritra Banerjee (Nokia)
K Tirumaleswar Reddy (Nokia)

Since IETF 122 Bangkok

- Both the drafts have been adopted by the WG
- HPKE WG formed at IETF 122, references updated to conform with the draft-ietf-hpke-pq
- IANA considerations updated

Transition Path to Post-Quantum EAP-AKA’



FIPS 203 (ML-KEM) is a new PQC KEM.
Hybrid can be used as defense in depth strategy (during the transition period).

PQ/T Hybrid enhancements for EAP-AKA’

https://datatracker.ietf.org/doc/draft-ietf-emu-hybrid-pqc-eapaka/

HPKE

- The HPKE specification provides a variant of public key encryption of arbitrary-sized plaintexts for a recipient public key.

- HPKE (Hybrid Public Key Encryption) emerged in the IETF as a prominent public key encryption scheme
  - https://www.rfc-editor.org/rfc/rfc9180.html (Developed by CFRG in IRTF)
  - Used by several protocols Oblivious HTTP, Encrypted Client Hello in TLS, MLS and COSE/JOSE

- HPKE interfaces are friendly to hybrid encryption (draft-ietf-hpke-pq & draft-irtf-cfrg-hybrid-kems)

Overview

- A new attribute, AT_PUB_HYBRID, is defined to carry the public key, which is the concatenation of traditional and PQC KEM public keys from the EAP server.
- The AT_PUB_HYBRID attribute will carry the encapsulated key, which is formed by concatenating the encapsulated key (enc) from the traditional KEM algorithm and the ciphertext (ct) from the PQC KEM Encapsulation function from the EAP peer.
- The AT_KDF_FS attribute is updated to indicate the HPKE KEM and HKDF (draft-ietf-hpke-pq and HKDF-SHA256) for generating the Hybrid Master Key MK_HYBRID.
- The Hybrid key derivation function will be included first in the EAP-Request to indicate a higher priority than the traditional key derivation function.

IANA considerations

Value	Description	Reference
TBA2	QSF-KEM(ML-KEM-768,P-256)-XOF(SHAKE256)-KDF(SHA3-256)	[TBD BY IANA: THIS RFC]
TBA3	KitchenSink-KEM(ML-KEM-768,X25519)-XOF(SHAKE256)-KDF(HKDF-SHA-256)	[TBD BY IANA: THIS RFC]

Post Quantum KEM mechanisms for EAP-AKA’

https://datatracker.ietf.org/doc/draft-ietf-emu-pqc-eapaka/

PQ Key Encapsulation Mechanism (KEMs)

- Key Encapsulation Mechanism (KEM) can be any asymmetric cryptographic scheme comprised of algorithms satisfying the following interfaces [PQCAPI].
  - def kemKeyGen() -> (pk, sk)
  - def kemEncaps(pk) -> (ct, ss)
  - def kemDecaps(ct, sk) -> ss

  where pk is public key, sk is secret key, ct is the ciphertext representing an encapsulated key, and ss is shared secret.

Overview

- A new attribute, AT_PUB_KEM, is defined to carry the PQC KEM public key from the EAP server.
- The AT_KEM_CT attribute will carry the ciphertext (ct) from the PQC KEM Encapsulation function from the EAP peer.
- The AT_KDF_FS attribute is updated to indicate the PQC KEM (MLKEM768) for generating the PQC Master Key MK_PQ_SHARED_SECRET.
- The PQC KEM will be included first in the EAP-Request to indicate a higher priority than the traditional key derivation function.

IANA considerations

Value	Description	Reference
TBA3	EAP-AKA' with MLKEM512	[TBD BY IANA: THIS RFC]
TBA4	EAP-AKA' with MLKEM768	[TBD BY IANA: THIS RFC]
TBA5	EAP-AKA' with MLKEM1024	[TBD BY IANA: THIS RFC]

Next Steps

- Adopted by the WG after IETF 122 Bangkok
- Request for reviews and suggestions