Post-Quantum Cryptography for Engineers

draft-ietf-pquip-pqc-engineers-02

IETF 118, PQUIP, 10th Nov 2023

Aritra Banerjee (Nokia)

Tiru Reddy (Nokia)

Dimitrios Schoinianakis (Nokia)

Tim Hollebeek (DigiCert)

Quick Recap of the draft

- The draft explains why engineers need to be aware of and understand post-quantum cryptography.

- It emphasizes the potential impact of Cryptographically Relevant Quantum Computers (CRQCs) on current cryptographic systems and the need to transition to post-quantum algorithms to ensure long-term security.

- Adopted by the WG following IETF 117

Changes since IETF 117

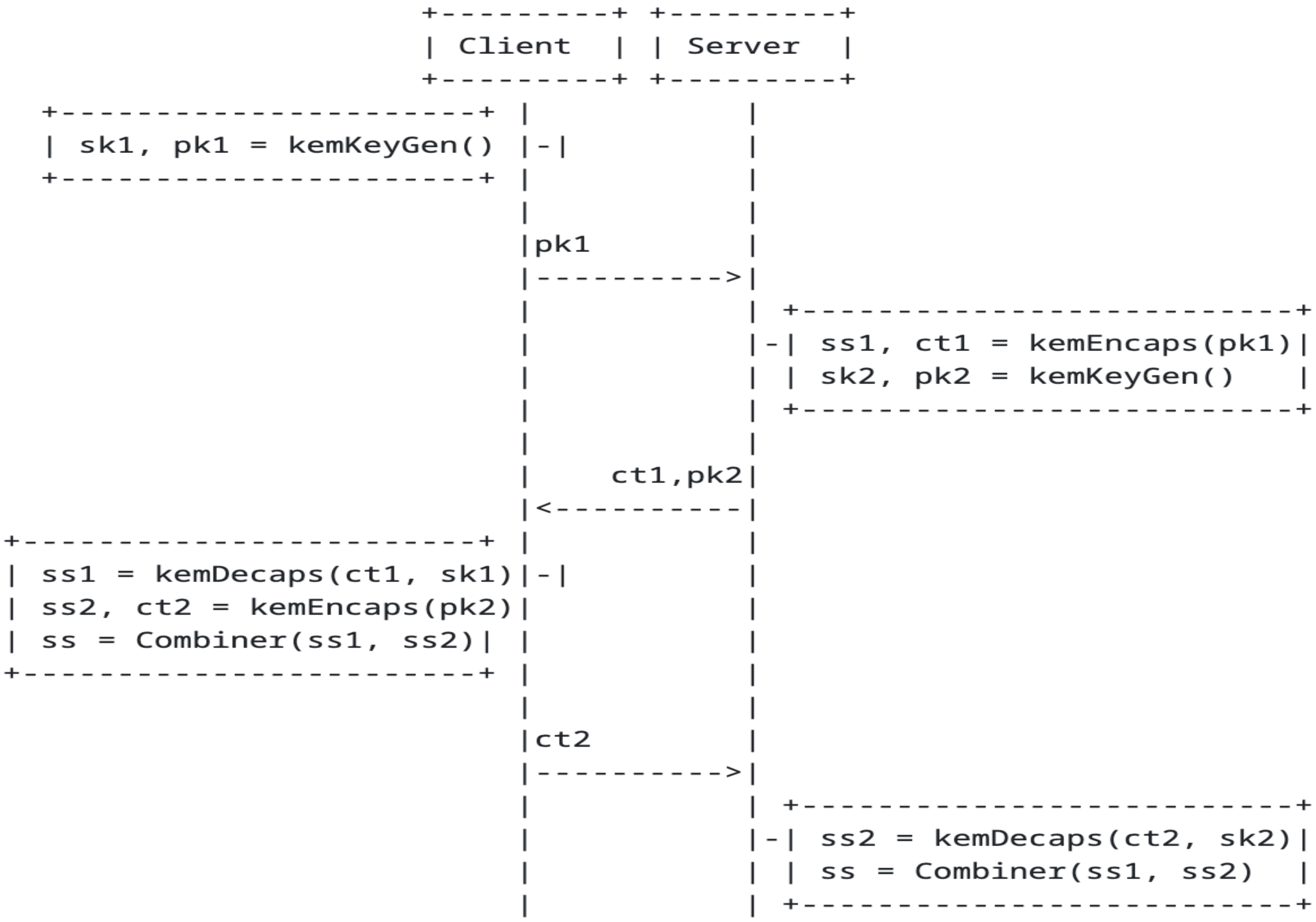
- Added Authenticated Key Exchange (AKE) subsection.

- Both the terms Post-Quantum vs Quantum Ready/Resistant are added to the draft.

- IKEv2 cannot fragment packets in the initial key exchange.
  - Added details of RFC9242 (IKEv2) which introduced an intermediate message exchange which can carry the PQ key exchanges and can be fragmented because of large public key sizes

KEM based AKE

- To achieve an AKE with KEM primitives, two full KEM exchanges need to be performed, and their results combined to form a single shared secret.
- Unlike DH which has NIKE + AKE property.
- Combiner complexity depends on cryptography properties required.



```
                      +---------+ +---------+
                      | Client  | | Server  |
                      +---------+ +---------+
  +----------------------+ |           |
  | sk1, pk1 = kemKeyGen() |-|         |
  +----------------------+ |           |
                           |           |
                           |pk1        |
                           |---------->|
                           |           | +--------------------------+
                           |           |-| ss1, ct1 = kemEncaps(pk1)|
                           |           | | sk2, pk2 = kemKeyGen()   |
                           |           | +--------------------------+
                           |           |
                           |    ct1,pk2|
                           |<----------|
+------------------------+ |           |
| ss1 = kemDecaps(ct1, sk1)|-|         |
| ss2, ct2 = kemEncaps(pk2)|           |
| ss = Combiner(ss1, ss2)| |           |
+------------------------+ |           |
                           |           |
                           |ct2        |
                           |---------->|
                           |           | +--------------------------+
                           |           |-| ss2 = kemDecaps(ct2, sk2)|
                           |           | | ss = Combiner(ss1, ss2)  |
                           |           | +--------------------------+
```

WG Discussion & Open Questions

- Name change of Kyber, Dilithium and SPHINCS+ to ML-KEM, ML-DSA, and SLH-DSA.
  - We would like change the names
  - But wait for Falcon FIPS draft for the new name for Falcon
  - Any objections ?

WG Discussion & Open Questions (Cont.)

- Hardware acceleration for PQC KEMs. A section/subsection to be added?
    - WG suggestion. Open to discussion.

Initial Changes after the 118 meeting

- Stateful hash-based signatures (XMSS and HSS/LMS) sizes to be also provided as a comparison to SPHINCS+
- RSA 10 seconds (stable qubit breaking RSA 2048) point to be removed (no academic reference) suggested in the WG
- Point on quantum side channel attack to be removed suggested in WG

Next Steps

- Addressing open issues

- Request WGLC after IETF 119, Brisbane

Contributing to this document

- Comments and Suggestions are welcome. Raise a PR and contribute.
- Thanks to all the Contributors and Reviewers.
- The document is being collaborated on: tireddy2/pqc-for-engineers (github.com)
- E-mail archive: pqc (ietf.org)