



IETF Hackathon

Post-Quantum Encrypted Client Hello

IETF 118

4–5 November 2023

Prague, Czech Republic



Hackathon Plan

- Making TLS 1.3 Extension “Encrypted Client Hello” *Quantum-Resistant*
- RFC’s and drafts involved:
 - [RFC 8446](#) - TLS version 1.3
 - [RFC 9180](#) - Hybrid Public Key Encryption (HPKE)
 - [draft-ietf-tls-esni-17](#) - Extension Encrypted Client Hello
- Used WolfSSL + liboqs as our base implementation
- Added *Post-Quantum* algorithms in HPKE and eventually in ECH
- PQ-ECH is still work in progress...

What got done

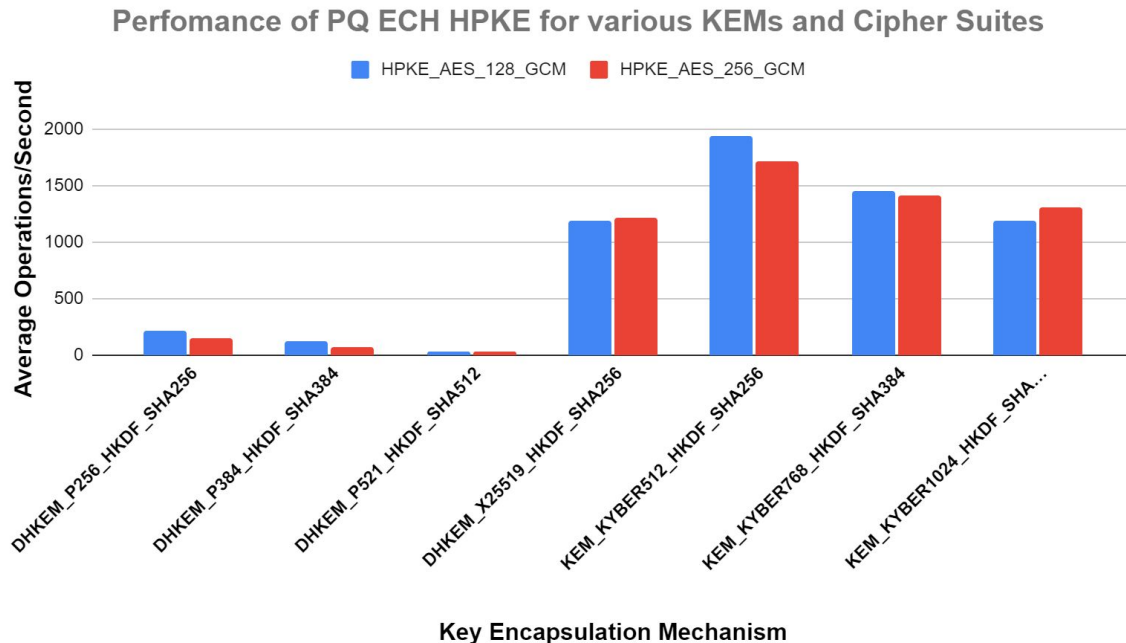
- Made HPKE run with Post-Quantum algorithms
 - Measured the performance of PQ-HPKE

Issues to resolve:

- PQC key sizes significantly bigger
- PQ KEMs (Kyber) different operation compared to traditional ECDH based KEMs (key exchange)
- It is still a work in progress...
 - Full ECH PQ extension

What we learned

- Compared PQ algorithms for various KEMs and Cipher Suites
- PQ algorithms run **significantly** faster
 - At least for HPKE



Wrap Up



Team members:

Dr. Apostolos Fournaris
George Tasopoulos
Dr. Evangelos Haleplidis

First timers @ IETF/Hackathon:

Apostolos Fournaris

Contacts:

fournaris@athenarc.gr
g.tasop@isi.gr
haleplidis@isi.gr

*Industrial Systems Institute,
Research Center ATHENA,
Greece*

This work has received funding from the European Union's Horizon H2020 project EnerMan and Horizon Europe research and innovation programme SecOPERA under grant agreement and No 958478 and No 101070599 respectively

IETF Hackathon - PQ-ECH

