COSE PQC

IETF 124 Hackathon
Montréal, 1-2 November 2025

Hackathon Plan

- The COSE working group is currently working on the integration of several PQC algorithms, including
  - **ML-DSA for JOSE and COSE**
  - **FN-DSA for JOSE and COSE**
  - **SLH-DSA for JOSE and COSE**
- Why not add them to the t_cose library?
- Use COSE ML-DSA as a warm-up exercise.
- Test vectors could be added to the drafts.

Results and Learned Lessons

- As a starting point I used work by Elonë Krasniqi. Thanks!
- Uses liboqs for the PQC algorithms.
  - Most likely not useful for IoT implementations.
- Took longer than expected
  - Was hoping that the coding would be faster with AI.
  - The integration of different crypto libraries in t_cose adds a bit of overhead and complexity.
- Will publish (polished) code at https://github.com/laurencelundblade/t_cose

Summary

- Team member:
  - Hannes Tschofenig (remote this time)

- Next steps:
  - Implement the rest of the algorithms.
  - Join the PQC X.509 team and add automated testing
  - Find others to test my COSE PQC code.