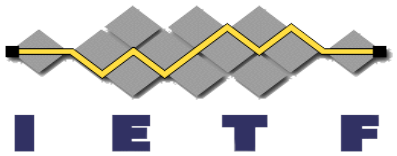
ML-KEM Security Considerations



draft-sfluhrer-cfrg-ml-kem-security-considerations

Scott Fluhrer, Quynh Dang, John Preuß Mattsson, Kevin Milner, Daniel Shiu
(and anyone else who wants to contribute)

IETF 121, Dublin

The purpose of this draft

This draft is intended to give guidance to protocol designers and implementors about how to use ML-KEM.

- It is intended for non-cryptosavvy readers
- It tries to give straight-forward actionable advice.
  - Nothing in this draft should be at all controversial to anyone here
  - It is here to give best practices for using ML-KEM

It is open for anyone in the CFRG to contribute..

The state of this draft

We have put together a first cut

- I believe that it’s in a decent basic state, but improvements can certainly be made
- There have been a number of edits since the quiet period started; mostly word-smithing, fixing typo’s and moving things between sections.

One Concern of Mine

People will end up using ML-KEM in lots of different ways

How much should it talk about the various use cases?

- Key exchange is easy (and pretty much is there)
- Public key encryption – it should be more explicit about RFC9180 (although ML-KEM parameter sets would be nice)
- Anything else (such as authentication)? I don't know what guidance to give

Next Steps

I ask that this be made a research group item

- I believe there is an immediate need for ML-KEM
- We need to give protocol designers advice now (before they freeze their design decisions in RFCs)