draft-fluhrer-cfrg-ntru-00 — WHY?

Reason: Kyber has some plausible patent claims

NIST is working with the patent holders to allow free access

However, it is unknown whether those agreements will be acceptable to everyone

The draft is here just in case it isn’t

Why NTRU?

- It is believed to be secure (as secure as Kyber)
  - NIST lists NTRU as its backup plan if it cannot reach licensing agreements
- It performs fairly well
- It is patent-free (all the NTRU patents have expired)

Goals of the draft

- Define NTRU
  - We can’t rely on NIST to do the work for us
  - We’re following the Round 3 NTRU submission
- Explain it in language accessible to engineers
- Facilitate interoperable implementations, and its use within protocols

Questions for the Research Group:

- Agree with this approach?
  - Until we see the licensing agreements, just saying ‘Kyber is the solution’ is not sufficient
- Issues with the draft?
- What is missing from the draft?
  - Test vectors, obviously, what else…