PQ KEMS DISCUSSION POINTS

- Problem Definition: Are we convinced that the problem being solved by adopting a PQ KEM for CFRG is well-defined and well-motivated?
- Appropriateness of Venue: Is the CFRG the right venue to pursue this work? Is specifying algorithms defined elsewhere a good use of the research group’s time?
- Need for Requirements Draft: Do we need a KEM requirements document before proceeding with any specific KEM adoption?
- Selection Criteria Without Requirements: If we decide not to write a separate requirements draft, how will the group evaluate and select among multiple KEM proposals for adoption?
- Alternatives approaches: Do protocol engineers have the tools necessary to make decisions around which KEM to incorporate in their protocol? Is this something the CFRG can help improve with with a meta-analysis?