Guidelines for Submitting Tweaks for 2nd Round Digital Signatures Candidates

Deadline: ~~January 17, 2025~~ Extended to February 5, 2025

Candidate teams must meet the same submission requirements and minimum acceptability criteria stated in the original Call for Proposals. Submissions must be submitted to NIST at pqc-submissions@nist.gov by February 5, 2025. Submissions should include a cover sheet, algorithm specifications (and other supporting documentation), and optical/digital media (e.g., implementations, known-answer test files, etc.) as described in the original Call For Proposals. In addition, NIST requires a short document outlining the modifications introduced in the new submission. This document should be included in the supporting documentation folder of the submission (see Section 2.C.3 of the CFP). NIST will review the proposed changes to determine whether they meet the submission requirements and minimum acceptability requirements, as well as whether they significantly affect the design of the algorithm and require a major reevaluation. As a general guideline, NIST expects any modifications to be relatively minor. It would be helpful if submission teams provided NIST with a summary of their expected changes prior to the deadline. If the deadline will pose a problem for any submission team, they should contact NIST in advance.

NIST does NOT need new signed IP statements unless new submission team members have been added, teams have merged, or the status of intellectual property for the submission has changed. If any of these cases apply, NIST will need new signed IP statements (see Section 2.D of the CFP). These statements may be provided electronically – and must be provided to NIST by the February 5 deadline. In particular, NIST will need new signed IP statements for members of the merged Mirath team.

NIST is aware that some submission packages may be large in size. The email system for pqc-submissions@nist.gov can only accept files up to 25MB. For larger files, candidate teams may upload submission packages at a location of their choosing and send NIST the download link. If that option is not suitable, NIST has a file transfer system that can be used (please email pqc-comments@nist.gov for more details). NIST will review the submitted packages as quickly as possible and post the candidate submission packages that are complete and proper on https://csrc.nist.gov/projects/pqc-dig-sig. Teams are encouraged to submit early. General questions may be asked on the pqc-forum. For more specific questions, please email pqc-comments@nist.gov.

The NIST PQC team