Guidelines for submitting tweaks for 2nd Round candidates

Deadline: March 15, 2019

As stated in the original Call for Proposals (CFP):

> Before the start of a second evaluation period, the submitters of the algorithms will have the option of providing updated optimized implementations for use during the next phase of the evaluation. During the course of the initial evaluations, it is conceivable that some small deficiencies may be identified in even some of the most promising submissions. Therefore, for the second round of evaluations, small modifications to the submitted algorithms will be permitted for either security or efficiency purposes. Submitters may submit minor changes (no substantial redesigns), along with a supporting justification that must be received by NIST prior to the beginning of the second evaluation period. (Submitters will be notified by NIST of the exact deadline.) NIST will determine whether the proposed modification would significantly affect the design of the algorithm, requiring a major re-evaluation; if such is the case, the modification will not be accepted. If modifications are submitted, new reference and optimized implementations and written descriptions must also be provided by the announced deadline. This will allow a thorough public review of the modified algorithms during the entire course of the second evaluation phase.

Candidate teams must meet the same submission requirements and minimum acceptability criteria as given in the original Call for Proposals. Submissions must be submitted to NIST at pqc-submissions@nist.gov by March 15, 2019. If this deadline will pose a problem for any submission team, we ask that they contact us. In particular, submissions should include a cover sheet, algorithm specifications (and other supporting documentation), and optical/digital media (implementations, known-answer test files, etc.) as described in Section 2 of CFP.

NIST does NOT need new signed IP statements, unless new submission team members have been added, or the status of intellectual property for the submission has changed. If either of these cases apply, NIST will need new signed IP statements (see Section 2.D of the CFP). These statements must be actual hard copies, not digital scans, and must be provided to NIST by the 2nd NIST PQC Standardization Conference.

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.4 of the CFP). NIST will review the proposed changes to see if they meet the submission requirements, minimum acceptability requirements, as well as if they would significantly affect the design of the algorithm requiring a major re-evaluation.

For merged teams (LEDAcrypt, NTRU, ROLLO, and Round5), the full submission package is also due on March 15, 2019 and must meet the same submission requirements and minimum acceptability requirements as stated in the CFP. NIST will need new signed statements (see Section 2.D of the CFP) from all team members, which must be given to NIST by the 2nd NIST PQC Standardization Workshop. As part of the submission package, NIST requires a brief document which highlights which aspects of each of the merged scheme are used. NIST will review the submission package to determine if it meets the submission requirements, minimum acceptability criteria, and the merged cryptosystem is in the span of the two original submissions (NIST does not want substantial re-designs).

As performance will play a larger role in the second round, NIST offers the following guidance. Submitters must include the reference and optimized implementation (which can be the same) with their submission package. The reference implementation should still be in ANSI C, however the optimized implementation is not required to be in ANSI C. NIST strongly recommends also providing an AVX2 (Haswell) optimized implementation, and in addition would encourage other optimized software implementations (e.g. microcontrollers) and hardware implementations (e.g. FPGAs).

We are aware that some submission packages may be large in size. Our email system for pqc-submissions@nist.gov is only set to handle files up to 25MB. For files which are larger, you may upload your submission package somewhere of your choosing and send us the download link when you submit. If that option isn't suitable, we do have a file transfer system that we can use. To find out about this option, please send us a message at pqc-comments@nist.gov.

NIST will review the submitted packages as quickly as possible and post the candidate submission packages which are "complete and proper" on our webpage www.nist.gov/pqcrypto. Teams are encouraged to submit early. General questions may be asked on the pqc-forum. For more specific questions, please contact us at pqc-comments@nist.gov.

The NIST PQC team