Announcement

It has been almost a year and a half since the second round of the NIST PQC Standardization Process began. After careful consideration, NIST would like to announce the candidates that will be moving on to the third round. The seven third-round Finalists are:

Third Round Finalists

Public-Key Encryption/KEMs	Digital Signatures
Classic McEliece	CRYSTALS-DILITHIUM
CRYSTALS-KYBER	FALCON
NTRU	Rainbow
SABER	

In addition, the following eight candidate algorithms will advance to the third round:

Alternate Candidates

Public-Key Encryption/KEMs	Digital Signatures
BIKE	GeMSS
FrodoKEM	Picnic
HQC	SPHINCS+
NTRU Prime	
SIKE	

During the third round, the term "finalist" will refer to the first seven algorithms listed above, and the terms "alternate" or "alternate candidate" will be used for the other eight algorithms also advancing. The finalists will continue to be reviewed for consideration for standardization at the conclusion of the third round. As CRYSTALS-KYBER, NTRU, and SABER are all structured lattice schemes, NIST intends to select, at most, one for the standard. The same is true for the signature schemes CRYSTALS-DILITHIUM and FALCON. In NIST's current view, these structured lattice schemes appear to be the most promising general-purpose algorithms for public-key encryption/KEM and digital signature schemes.

For the eight alternate candidate algorithms being advanced into the third round, NIST notes that these algorithms may still potentially be standardized, although that most likely will not occur at the end of the third round. NIST expects to have a fourth round of evaluation for some of the candidates on this track. Several of these alternate candidates have worse performance than the finalists but might be selected for standardization based on a high confidence in their security. Other candidates have acceptable performance but require additional analysis or other work to inspire sufficient confidence in their security or security rationale. In addition, some alternates were selected based on NIST's desire for a broader range of hardness assumptions in future post-quantum security standards, their suitability for targeted use cases, or their potential for further improvement.

NIST would like to thank all of the submission teams for their efforts in this standardization process. It was not an easy decision to narrow down the submissions. A detailed description of the decision process and rationale for selection will be available in NIST Internal Report

(NISTIR) 8309, *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. It will soon be available at https://csrc.nist.gov/publications and on the NIST post-quantum webpage www.nist.gov/pqcrypto. Questions may be directed to pqc-comments@nist.gov. NIST hopes that the teams whose scheme were not selected to advance will continue to participate by evaluating and analyzing the remaining cryptosystems along with the cryptographic community at large. These combined efforts are crucial to the development of NIST's future post-quantum public-key standards.

For the algorithms moving on to the third round, NIST will allow the submission teams the option of providing updated specifications and implementations (i.e., "tweaks"). The deadline for these tweaks will be October 1, 2020. It would be helpful if submission teams provided NIST with a summary of their expected changes by August 10, 2020. If any submission team feels that they may not meet the deadlines, they are strongly encouraged to contact NIST to discuss. NIST will review the proposed modifications and publish the accepted submissions shortly afterwards. As a general guideline, NIST expects that any modifications to the seven finalists will be relatively minor while allowing more latitude to the eight alternate candidate algorithms. Note, however, that larger changes may signal that an algorithm is not mature enough for standardization at this time. More detailed information and guidance will be provided in another message.

It is estimated that this third phase of evaluation and review will last 12-18 months. NIST is planning to hold a 3rd NIST PQC Standardization Conference in 2021. Obviously, much of the conference details will depend on conditions relating to the pandemic and have not been finalized. The preliminary Call for Papers for this conference can be found at www.nist.gov/pqcrypto and will also be posted to this pqc-forum in another message. The deadline for submission to the 3rd NIST PQC Conference will likely be sometime around the end of 2020.

The NIST PQC team

Note: These are NIST's current plans. If new results emerge during the third round which undermine NIST's confidence in some of the finalists, NIST may extend the timeline, or make changes to the process. If NIST has less serious concerns specific to a particular finalist and sees the need to continue evaluating it, NIST may instead defer the decision about standardization for the affected finalist until the fourth round.

---------- END ROUND 3 "ANNOUNCEMENT" ----------

Guidelines for submitting tweaks for Third Round Finalists and Candidates
Deadline: October 1, 2020

Finalist and 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 October 1, 2020. It would be helpful if submission teams provided NIST with a summary of their expected changes by August 10, 2020. If either of these deadlines will pose a problem for any submission team, they should contact NIST in advance. In particular, 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 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 3rd NIST PQC Standardization Conference. In particular, NIST will need new signed IP statements for new members of the merged Classic McEliece team.

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 and minimum acceptability requirements, as well as if they would significantly affect the design of the algorithm, requiring a major re-evaluation. As a general guideline, NIST expects any modifications to the seven finalists to be relatively minor while allowing more latitude to the eight alternate candidate algorithms. Note, however, that larger changes may signal that an algorithm is not mature enough for standardization for some time.

As performance will continue to play a large role in the third 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 would encourage other optimized software implementations (e.g. microcontrollers) and hardware implementations (e.g. FPGAs).

NIST is aware that some submission packages may be large in size. The 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 is not suitable, NIST has a file transfer system that can be used. To find out about this option, please send a message to 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

CFP for 3rd workshop

Call for Papers for the 3rd NIST PQC Standardization Conference
Location: To be determined
Spring or Summer 2021 (Tentatively)
Submission deadline: Will be announced. Sometime around the end of 2020.
(Conference without proceedings)

The NIST Post-Quantum Cryptography Standardization Process has entered the third round in which seven finalists are being considered for initial standardization in addition to eight alternate candidate algorithms, which are also advancing to the third round. NIST plans to hold the 3rd NIST PQC Standardization Conference in the spring of 2021 to discuss various aspects of these algorithms and to obtain valuable feedback for informing decisions on standardization. NIST will invite each of the seven finalist submission teams to give an update on their algorithms, as well as time for the eight alternate candidate teams to present.

In addition, NIST is soliciting research and discussion papers, surveys, presentations, case studies, panel proposals, and participation from all interested parties, including researchers, system architects, implementors, vendors, and users. NIST will post the accepted papers and presentations on the conference website after the conference; however, no formal proceedings will be published. NIST encourages the submission of presentations and reports on preliminary work that participants plan to publish elsewhere.

Topics for submissions should include but are not limited to:

- Classical and quantum cryptanalysis of finalists/candidates, including cryptanalysis of weakened or toy versions
- Analysis of relative performance or resource requirements for some or all of the finalists/candidates
- Assessments of classical and quantum security strengths of the finalist/candidate algorithms
- Systemization of knowledge relevant to the NIST PQC standardization process
- Substantial improvements in the implementation of finalists/candidates
- Improved analysis or proofs of properties of finalists/candidates, even when this does not lead to any attack
- Proposed criteria to be used for selecting algorithms for standardization
- Impacts to existing applications and protocols (e.g., changes needed to accommodate specific algorithms)
- Steps or strategies for organizations to prepare for the coming transition

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x 11 inches). Submitted papers must not exceed 20 pages, excluding references and appendices (single space, with 1-inch margins using a 10 pt or larger font). Proposals for panels should be no longer than five pages and should include possible panelists and an indication of which panelists have confirmed their participation.

Please submit the following information to pqc2021@nist.gov:

- Name, affiliation, email, phone number (optional), postal address (optional) for the primary submitter
- First name, last name, and affiliation of each co-submitter
- Finished paper, presentation, or panel proposal in PDF format as an attachment

All submissions will be acknowledged.

General information about the conference, including registration and accommodation information, will be available at the conference website: http://www.nist.gov/pqcrypto.