Call for Papers for the 3rd NIST PQC Standardization Conference

Location: Virtual
June 7-9, 2021* (save the date)
Submission deadline: April 23, 2021
Notification date: May 7, 2021

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 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/alternates, including cryptanalysis of weakened or toy versions
- Analysis of relative performance or resource requirements for some or all of the finalists/alternates
- Assessments of classical and quantum security strengths of the finalist/alternate algorithms
- Systemization of knowledge relevant to the NIST PQC standardization process
- Substantial improvements in the implementation of finalists/alternates
- Improved analysis or proofs of properties of finalists/alternates, 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.

** June 7-9 is the projected date for the conference. We are still finalizing some of the logistical details. We do not anticipate any issues which will change the dates, but haven't yet received final authorization.*