Call for Papers for the 2nd NIST PQC Standardization Conference

Santa Barbara, CA
August 22 – 24, 2019
Submission deadline: May 31, 2019 (Conference without proceedings)

The NIST Post-Quantum Cryptography Standardization Process has entered the next phase, in which 26 second-round candidates are being considered for standardization. NIST plans to hold a second NIST PQC Standardization Conference in August 2019 to discuss various aspects of these candidates, and to obtain valuable feedback for the selection of the finalists soon after the conference. NIST will invite each submission team of the 26 second-round candidates to give a short update on their algorithm.

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. To avoid the possible duplication of papers and presentations accepted for this conference and for Crypto and affiliated events, which are held consecutively, submissions will NOT be considered for this conference if they are substantially similar to the submissions accepted for Crypto 2019 or included in the program of other affiliated events.

Topics for submissions should include, but are not limited to, the following:

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

Deadlines:

- **Submission Deadline: May 31, 2019**
- **Authors Notified: June 21, 2019**
- **Final Version Deadline: July 19, 2019**

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 **pqc2019@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
- The finished paper, presentation, or panel proposal in PDF format as an attachment.

All submissions will be acknowledged.

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