Call for Papers for the 5th NIST PQC Standardization Conference

Location: Hilton Washington DC/Rockville Hotel in Rockville, Maryland
April 10-12, 2024
Submission deadline: Friday, January 26th, 2024
(Conference without proceedings)

NIST plans to hold the 5th NIST PQC Standardization Conference from April 10-12, 2024, in Rockville, Maryland. The purpose of the conference is to discuss various aspects of the algorithms (both those selected and those being evaluated) and to obtain valuable feedback for informing decisions on standardization. NIST will invite the submission teams for BIKE, Classic McEliece, Falcon, and HQC to give an update on their algorithms.

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 the algorithms, including cryptanalysis of weakened or toy versions
- Analysis of relative performance or resource requirements for some or all of the algorithms
- Assessments of classical and quantum security strengths of the algorithms
- Systemization of knowledge relevant to the NIST PQC standardization process
- Substantial improvements in the implementation of algorithms
- Improved analysis or proofs of properties of the selected algorithms/candidates, even when this does not lead to any attack
- Proposed criteria to be used for selecting algorithms for standardization
- Testing and validations of implementations of PQC algorithms
- 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 pqc2024@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 information, will be available at the conference website: http://www.nist.gov/pqcrypto.