Call for Submissions - NIST Workshop on Guidance for KEMs
February 25-26, 2025
(Virtual Event Only)
Submission Deadline: January 28, 2025

NIST recently published FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, to update its cryptographic standards with an algorithm designed to provide protection from quantum attacks. In addition, NIST will select one or two additional quantum-resistant key encapsulation mechanisms (KEMs) for standardization. To provide guidance on using KEMs, NIST has released draft NIST SP 800-227, *Recommendations for Key Encapsulation Mechanisms*. Public comments on SP 800-227 are due by March 7, 2025.

To further engage the cryptographic community and gather feedback, NIST will hold a virtual workshop on **February 25-26, 2025**, focusing on draft SP 800-227. The workshop aims to facilitate discussions on NIST's guidance for KEMs.

NIST invites submissions in the form of discussion papers, surveys, presentations, research, case studies, panel proposals, and participation from all interested parties, including researchers, system architects, implementors, vendors, and users. NIST will post any accepted submissions on the conference website after the conference; however, no formal proceedings will be published.

Topics for submissions should include but are not limited to:

- Testing and validations of implementations of KEMs
- Impacts to existing applications and protocols (e.g., changes needed to accommodate KEMs)
- Steps or strategies for organizations to prepare for migrating to KEMs
- Input checking for values input to KEM algorithms
- Using KEMs for authenticated key establishment
- Key combiners for KEMs, or hybrid/composite KEMs
- Performance, scalability, or interoperability considerations for KEM deployment
- Implementation experiences and lessons learned from KEM adoption
- Potential use cases and industry applications of KEMs
- Limits for use of ephemeral keys

Additional relevant topics are welcome.

Submissions should be provided electronically, in PDF or PowerPoint format. As there is a short amount of time for this call, NIST is looking for extended abstracts of 1-2 pages describing what would be presented. Alternatively, slides of a proposed presentation could be submitted. Proposals for panels should include the topics for discussion, as well as possible panelists and an indication of which panelists have confirmed their participation.

Please submit the following information to pqc-kems2025@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
- Extended abstract, presentation, or panel proposal in electronic 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.