

Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process

2.A Cover Sheet

The cover sheet of a submission package shall contain the following information:

- Name of the proposed cryptosystem.
- Principal submitter's name, e-mail address, telephone, organization, and postal address.
- Name(s) of auxiliary submitter(s).
- Name of the inventor(s)/ developer(s) of the cryptosystem.
- Name of the owner, if any, of the cryptosystem (normally expected to be the same as the submitter).
- Signature of the submitter.
- (optional) Backup point of contact (with telephone, fax, postal address, and e-mail address).

2.B Algorithm Specifications and Supporting Documentation

Each submission must include:

- 1) a complete written specification
- 2) a detailed performance analysis
- 3) Known Answer Test values
- 4) a thorough description of the expected security strength
- 5) an analysis of the algorithm with respect to known attacks
- 6) a statement of advantages and limitations.

2.C Digital and Optical Media

All electronic data shall be provided either in a zip file, or on a single CD-ROM, DVD, or USB flash drive labeled with the submitter's name, as well as the name of the proposed cryptosystem.

Further details are included in the full [Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process](#).