Panel: Rehashing Pre-Hashing

Submitter: Burt Kaliski, Verisign
Updated April 1, 2024

Abstract

The draft FIPS 204 and 205 include an option to apply the signature scheme to the digest (i.e., hash) of a message rather than the message itself, in order to reduce the size of the message input to the signature and verification operations. Several of the public comments[1] [2] on the drafts addressed the pre-hashing step that would produce the digest to be signed and how it would be used in applications. NIST followed up on the pqc-forum mailing list with a note, "Pure vs. pre-hash signing for ML-DSA and SLH-DSA," [3] proposing a way to format the message input to the signature scheme in a way that distinguishes digest inputs from regular inputs. Participants responded to NIST's proposal with further comments.[4]

With the draft standards reaching their final form, it would be helpful to have a broader discussion on the design considerations for pre-hashing and how they may affect both the specification and the usage of FIPS 204 and 205.

Panel Questions

1. Should FIPS 204 and 205 specify an optional pre-hashing step? Alternatively, should NIST provide guidance in a Special Publication?
2. If not, should NIST encourage development of a general-purpose specification and/or guidance for pre-hashing in other standards development organizations?
3. Or, would it be preferable to have special-purpose specifications and/or guidance developed by the protocols and use cases that employ a pre-hashing option?
4. What are some examples of the protocols and use cases that might employ a pre-hashing option? What is their rationale?
5. Should randomized hashing be included as an option in the guidance or specification?
6. What about other inputs, such as the signer's public key?
7. What other kinds of usage guidance for pre-hashing messages would be helpful to have?

Moderator

- John Kelsey, NIST

Panelists

- Scott Fluhrer, Cisco
- Joseph Harvey, Verisign
- Markku-Juhani O. Saarinen, SoC Hub Research Centre, Tampere University, Finland

[1] https://csrc.nist.gov/files/pubs/fips/204/ipd/docs/fips-204-initial-public-comments-2023.pdf
[2] https://csrc.nist.gov/files/pubs/fips/205/ipd/docs/fips-205-initial-public-comments-2023.pdf
[3] https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/qsmP_5ZZx0g/m/_UJptbmXAgAJ
[4] https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/qsmP_5ZZx0g/m/7IT2jD69AAAJ