# SHAKE128/256 and SHAKE256/512 for PKIX and S/MIME

Quynh Dang
Computer Security Division
National Institute of Standards and Technology (NIST)

-**Specifying SHAKE128/256 and SHAKE256/512 for PKIX and S/MIME.**
Supporting reason: Keccak and SHA-3 functions (including all the FIPS 202 and SP 800-185 functions) are the outcome of an open competition, unlike the previous hashing standards. They have a clear design rationale and have been receiving a lot of public cryptanalysis during and after the SHA-3 competition to today. All of that gives great confidence that the SHA-3s are very secure. The SHA3s also have much larger security margins than SHA-2s. In addition, since the design of the SHA3s is very different from SHA-2s (and other ARX-based designs), they offer sane diversity for security. Therefore, the SHA-3s are excellent alternatives to SHA2s.

December 2017: WG adoption of a SHAKE128/256 and SHAKE256/512 draft for PKIX.
December 2017: WG adoption of a SHAKE128/256 and SHAKE256/512 draft for S/MIME.
August 2018: WGLC for the SHAKE128/256 and SHAKE256/512 draft for PKIX.
August 2018: WGLC for the SHAKE128/256 and SHAKE256/512 draft for S/MIME.