

History of PQC Standardization Round 1 Updates:

February 20, 2018	Withdrawn Algorithm Edon-K Added Official Comment file: Lizard Updated Comment file: BIKE Edon-K LAC Ramstake
February 15, 2018	Updated Comment file: LAC
February 14, 2018	Added Official Comment file: Ramstake
February 13, 2018	Added Official Comment file: DAGS LIMA Updated Comment file: LEDAkem Lepton
February 12, 2018	Updated Comment file: Lepton <i>(originally submitted 12/29/2017 – but not as “Official Comment”)</i>
February 9, 2018	Updated Comment file: DRS LEDApkc
February 8, 2018	Added Official Comment file: LEDApkc
February 6, 2018	Updated Comment file: DRS pqsigRM WalnutDSA

History of PQC Standardization Round 1 Updates:

February 1, 2018	Updated Comment file: HILA5 Three Bears WalnutDSA
January 31, 2018	Added Official Comment File Three Bears Updated Comment file: HILA5 Added Submitter's Website NTRU Prime
January 24, 2018	Added Official Comment File NTRUEncrypt Updated Comment file: LAC WalnutDSA
January 23, 2018	Updated Comment file: CRYSTALS-KYBER pqsigRM WalnutDSA
January 18, 2018	Updated Comment file: HQC LAC pqsigRM WalnutDSA
January 17, 2018	Added Official Comment File CRYSTALS-KYBER HQC Updated Comment file: WalnutDSA

History of PQC Standardization Round 1 Updates:

January 16, 2018	<p>Added Official Comment File LAC WalnutDSA</p> <p>Updated Comment file: Compact LWE DME Round2</p> <p>Algorithm Files Replaced* Giophantus KINDI Three Bears</p> <p><i>*minor implementation fixes to be compatible with the NIST API, which were requested by NIST, and the only modifications allowed (were those small fixes). We tried to catch all these before we announced the Round 1 submissions, but we missed a few small things.</i></p>
January 12, 2018	<p>Added Official Comment file: Giophantus Round2</p> <p>Updated Comment file: DME Gravity-SPHINCS</p>
January 11, 2018	<p>Added Official Comment file: Gravity-SPHINCS HILA5 LEDAkem Odd Manhattan</p> <p>Updated Comment file: BIKE HK17 pqsigRM RaCoSS</p>

History of PQC Standardization Round 1 Updates:

January 9, 2018	<p>Withdrawn Algorithm HK17 SRTPI</p> <p>Added Official Comment file: CFPKM KCL (pka OKCN/AKCN/CNKE)</p> <p>Updated Comment file: HK17 LAKE LOCKER pqsigRM SRTPI</p>
January 8, 2018	<p>Withdrawn Algorithm RVB</p> <p>Added Official Comment file: BIKE Compact LWE CRYSTALS-DILITHIUM Edon-K LAKE Lepton LOCKER LOTUS pqsigRM RLCE-KEM SRTPI</p> <p>Updated Comment file: DME RVB</p> <p>Added submitter's website: NewHope</p>
January 4, 2018	<p>Renamed OKCN/AKCN/CNKE KCL (<i>which stands for "Key Consensus from Lattice"</i>)</p> <p>Added submitter's website: CRYSTALS-DILITHIUM CRYSTALS-KYBER LOTUS PICNIC pqsigRM</p>

History of PQC Standardization Round 1 Updates:

December 27, 2017	Added Official Comment file: DME DRS Guess Again HK17 McNie pqNTRUsign qTESLA RaCoSS RVB Added submitter's website: Giophantus KINDI
December 21, 2017	Initial Posting of Round 1 Algorithms (69)