

History of PQC Standardization Round 1 Updates:

January 28, 2019	Added Official Comment files: NTRU-HRSS-KEM Post-Quantum RSA-Encryption Titanium Updated comment files DME LAC Ramstake WalnutDSA
December 22, 2018 – January 25, 2019	Government Shutdown
December 19, 2018	Updated Comment file: DAGS
December 17, 2018	Added Official Comment File: RQC Updated Comment file: HQC NTRU Prime
December 10, 2018	Added Official Comment File: Rainbow Updated Comment file: KCL LAC
December 6, 2018	Added Official Comment File: Picnic
December 4, 2018	Added Official Comment File: NewHope Updated Comment file: LAC WalnutDSA

History of PQC Standardization Round 1 Updates:

December 3, 2018	Updated Comment files: DRS LAC Odd Manhattan SIKE WalnutDSA
November 29, 2018	Updated Comment file: LAC
November 28, 2018	Updated IP Statement SIKE (<i>added additional 2.D.2 Statement by Patent Owner</i>)
November 27, 2018	Updated Comment file: LAC
November 26, 2018	Updated Comment file: EMBLEM and R.EMBLEM LAC
November 20, 2018	Updated Comment file: LAC
November 19, 2018	Updated Comment file: LEDAkem LEDApkc
November 5, 2018	Updated Comment file: Gravity-SPHINCS SPHINCS+
October 29, 2018	Updated Comment file: HiMQ-3 Added Submitter's Website: GeMSS DualModeMS
October 24, 2018	Updated Comment file: HiMQ-3 LAC
October 23, 2018	Updated Comment file: NTRUPrime

History of PQC Standardization Round 1 Updates:

October 19, 2018	Updated Comment file: DME
October 11, 2018	Updated Comment file: pqsigRM
October 4, 2018	Updated Comment file: pqsigRM
October 1, 2018	Updated Comment file: Classic McEliece LEDAkem LEDApkc
September 20, 2018	Updated Comment file: CRYSTALS-DILITHIUM Lima
September 18, 2018	Updated Comment file: CRYSTALS-DILITHIUM
September 13, 2018	Updated Comment File: HiMQ-3
September 10, 2018	Updated Comment File: DualModeMS
September 4, 2018	Added Official Comment File and Submitter's Website: MQDSS
August 30, 2018	Updated Comment File: qTESLA
August 27, 2018	Updated Comment File: Round5
August 24, 2018	Added Official Comment File: DualModeMS
August 9, 2018	Updated Comment File: Round5

History of PQC Standardization Round 1 Updates:

August 7, 2018	Added Official Comment File: Round5 (<i>possible merger of HILA5 and Round2</i>) Updated Comment File: BIKE HiMQ-3
July 30, 2018	Updated Comment File: NTRUEncrypt
July 26, 2018	Updated Comment File: BIKE
July 18, 2018	Updated Comment File: HiMQ-3
July 11, 2018	Updated Comment File: NTRUEncrypt
July 5, 2018	Updated Comment File: NTS-KEM
July 3, 2018	Updated Comment File: Classic McEliece NTRUEncrypt qTESLA
June 27, 2018	Updated Comment File: NTRU Prime
June 25, 2018	Submitter's Website EMBLEM and R.EMBLEM
June 21, 2018	Updated Comment File: NTRU Prime
June 19, 2018	Updated Comment File: Gui KCL qTESLA Submitter's Website qTESLA
June 14, 2018	Updated Comment File: Giophantus

History of PQC Standardization Round 1 Updates:

June 13, 2018	Updated Comment File: pqsigRM
June 11, 2018	Updated Comment File: Giophantus Round2
June 6, 2018	Updated Comment File: NTRUEncrypt
June 5, 2018	Updated Comment File: pqsigRM
May 30, 2018	Updated Comment File: RLCE-KEM WalnutDSA
May 29, 2018	Added Official Comment File: Classic McEliece Updated Comment File: KCL Round2 SPHINCS+ WalnutDSA
May 24, 2018	Updated Comment File: SPHINCS+ WalnutDSA
May 18, 2018	Updated Comment File: NTRU Prime
May 16, 2018	Updated Comment File: DAGS
May 15, 2018	Updated Comment File: WalnutDSA
May 14, 2018	Updated Comment File: NTRU Prime IP Statements posted DualModeMS and GeMSS

History of PQC Standardization Round 1 Updates:

May 8, 2018	Updated Comment File: GeMMS
May 7, 2018	Added Official Comment File: HiMQ-3 Updated Comment File: NTRU Prime WalnutDSA IP Statements posted <i>Not yet received: DualModeMS and GeMSS</i>
May 1, 2018	Added Official Comment File: Gui GeMSS Updated Comment File: NTRU Prime
April 26, 2018	Added Official Comment File: NTS-KEM Updated Comment File: FrodoKEM NTRU Prime
April 23, 2018	Added Official Comment File: FrodoKEM Updated Comment File: NTRU Prime
April 20, 2018	Updated Comment File: DRS Submitter's Website WalnutDSA
April 18, 2018	Updated Comment File: Gravity-SPHINCS LAC SPHINCS+

History of PQC Standardization Round 1 Updates:

April 12, 2018	Added Official Comment File: EMBLEM and R.EMBLEM Updated Comment File: pqsigRM Submitter's Website: SIKE
April 11, 2018	Updated Comment file: CRYSTALS-Kyber HILA5 RLCE-KEM
April 9, 2018	Updated Comment file: NTRUEncrypt WalnutDSA
April 6, 2018	Updated Comment file: CRYSTALS-DILITHIUM NTRUEncrypt SIKE
April 5, 2018	Updated Comment file: pqsigRM SIKE WalnutDSA
April 4, 2018	Withdrawn Algorithm RankSign Added Official Comment file: RankSign Updated Comment file: SIKE
April 2, 2018	Updated Comment file: HILA5 pqsigRM SIKE

History of PQC Standardization Round 1 Updates:

March 29, 2018	Added Official Comment file: SIKE Updated Comment file: LAKE
March 28, 2018	Updated Comment file: DRS NTRU Prime
March 27, 2018	Updated Comment file: NTRU Prime pqNTRUSign
March 26, 2018	Updated Comment file: CRYSTALS-DILITHIUM NTRUEncrypt
March 23, 2018	Updated Comment file: HILA5
March 21, 2018	Updated Comment file: pqNTRUSign
March 19, 2018	Updated Comment file: pqNTRUSign Round 2
March 15, 2018	Updated Comment file: NTRU Prime
March 14, 2018	Added Official Comment file: SPHINCS+ Updated Comment file: NTRU Prime pqNTRUSign
March 12, 2018	Updated Comment file: BIKE pqNTRUSign
March 9, 2018	Updated Comment file: pqsigRM

History of PQC Standardization Round 1 Updates:

March 8, 2018	Added Official Comment file: NTRU Prime Updated Comment file: RaCoSS
February 28, 2018	Updated Comment file: Lizard
February 26, 2018	Updated Comment file: LAC
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

History of PQC Standardization Round 1 Updates:

February 8, 2018	Added Official Comment file: LEDApkc
February 6, 2018	Updated Comment file: DRS pqsigRM WalnutDSA
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	Withdrawn Algorithm HK17 SRTPI Added Official Comment file: CFPKM KCL (pka OKCN/AKCN/CNKE) Updated Comment file: HK17 LAKE LOCKER pqsigRM SRTPI
January 8, 2018	Withdrawn Algorithm RVB Added Official Comment file: BIKE Compact LWE CRYSTALS-DILITHIUM Edon-K LAKE Lepton LOCKER LOTUS pqsigRM RLCE-KEM SRTPI Updated Comment file: DME RVB Added submitter's website: NewHope
January 4, 2018	Renamed OKCN/AKCN/CNKE KCL (<i>which stands for "Key Consensus from Lattice"</i>) Added submitter's website: CRYSTALS-DILITHIUM CRYSTALS-KYBER LOTUS PICNIC pqsigRM

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)