Round 1 Submissions

Official comments on the First Round Candidate Algorithms should be submitted using the "Submit Comment" link for the appropriate algorithm. Comments from the pqc-forum Google group subscribers will also be forwarded to the pqc-forum Google group list. We will periodically post and update the comments received to the appropriate algorithm.

All relevant comments will be posted in their entirety and should not include PII information in the body of the email message.

Please refrain from using OFFICIAL COMMENT to ask administrative questions, which should be sent to pqc-comments@nist.gov

By selecting the "Submitter's Website" links, you will be leaving NIST.gov. We have provided links to submitter web sites because they may have information that would be of interest to you. No inferences should be drawn o.n account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites

History of Updates
* denotes algorithm has been withdrawn

Algorithm	Algorithm Information *KAT files are included in zip file unless they were too large*	Submitters	Comments
BIG QUAKE	Zip File (4MB) IP Statements Website	Alain Couvreur Magali Bardet Elise Barelli Olivier Blazy Rodolfo Canto-Torres Philippe Gaborit Ayoub Otmani Nicolas Sendrier Jean-Pierre Tillich	Submit Comment View Comments
BIKE	Zip File (10MB) IP Statements Website	Nicolas Aragon Paulo Barreto Slim Bettaieb Loic Bidoux Olivier Blazy Jean-Christophe	Submit Comment View Comments

		Deneuville Phillipe Gaborit Shay Gueron Tim Guneysu Carlos Aguilar Melchor Rafael Misoczki Edoardo Persichetti Nicolas Sendrier Jean-Pierre Tillich Gilles Zemor	
CFPKM	Zip File (<1MB) IP Statements Website	O. Chakraborty J.-C. Faugere L. Perret	Submit Comment View Comments
Classic McEliece	Zip File (<1MB) KAT Files (26MB) IP Statements Website	Daniel J. Bernstein Tung Chou Tanja Lange Ingo von Maurich Rafael Misoczki Ruben Niederhagen Edoardo Persichetti Christiane Peters Peter Schwabe Nicolas Sendrier Jakub Szefer Wen Wang	Submit Comment View Comments
Compact LWE	Zip File (1MB) IP Statements Website	Dongxi Liu Nan Li Jongkil Kim Surya Nepal	Submit Comment View Comments
CRYSTALS-DILITHIUM	Zip File (6MB) IP Statements Website	Vadim Lyubashevsky Leo Ducas Eike Kiltz Tancrede Lepoint Peter Schwabe Gregor Seiler Damien Stehle	Submit Comment View Comments
CRYSTALS-KYBER	Zip File (2MB) IP Statements Website	Peter Schwabe Roberto Avanzi Joppe Bos Leo Ducas Eike Kiltz Tancrede Lepoint Vadim Lyubashevsky John M. Schanck Gregor Seiler Damien Stehle	Submit Comment View Comments

DAGS	Zip File (1MB) KAT Files (18MB) IP Statements Website	Gustavo Banegas Paolo S. L. M. Barreto Brice Odilon Boidje Pierre-Louis Cayrel Gilbert Ndollane Dione Kris Gaj Cheikh Thiecoumba Gueye Richard Haeussler Jean Belo Klamti Ousmane N'diaye Duc Tri Nguyen Edoardo Persichetti Jefferson E. Ricardini	Submit Comment View Comments
Ding Key Exchange	Zip File (1MB) IP Statements Website	Jintai Ding Tsuyoshi Takagi Xinwei Gao Yuntao Wang	Submit Comment View Comments
DME	Zip File (1MB) IP Statements Website	Ignacio Luengo Martin Avendano Michael Marco	Submit Comment View Comments
DRS	Zip File (4MB) IP Statements Website	Thomas Plantard Arnaud Sipasseuth Cedric Dumondelle Willy Susilo	Submit Comment View Comments
DualModeMS	Zip File (1MB) KAT Files (20MB) IP Statements Website	J.-C. Faugere L. Perret J. Ryckeghem	Submit Comment View Comments
***Edon-K**	Zip File (16MB) IP Statements Website	Danilo Gligoroski Kristian Gjosteen	Submit Comment View Comments
EMBLEM and R.EMBLEM	Zip File (2MB) IP Statements Website	Minhye Seo Jong Hwan Park Dong Hoon Lee Suhri Kim Seung-Joon Lee	Submit Comment View Comments
FALCON	Zip File (55MB) IP Statements Website	Thomas Prest Pierre-Alain Fouque Jeffrey Hoffstein Paul Kirchner	Submit Comment View Comments

		Vadim Lyubashevsky Thomas Pornin Thomas Ricosset Gregor Seiler William Whyte Zhenfei Zhang	
FrodoKEM	Zip File (15MB) IP Statements Website	Michael Naehrig Erdem Alkim Joppe Bos Leo Ducas Karen Easterbrook Brian LaMacchia Patrick Longa Ilya Mironov Valeria Nikolaenko Christopher Peikert Ananth Raghunathan Douglas Stebila	Submit Comment View Comments
GeMSS	Zip File (2MB) KAT Files (54MB) IP Statements Website	A. Casanova J.-C. Faugere G. Macario-Rat J. Patarin L. Perret J. Ryckeghem	Submit Comment View Comments
Giophantus	Zip File (8MB) IP Statements Website	Koichiro Akiyama Yasuhiro Goto Shinya Okumura Tsuyoshi Takagi Koji Nuida Goichiro Hanaoka Hideo Shimizu Yasuhiko Ikematsu	Submit Comment View Comments
Gravity-SPHINCS	Zip File (8MB) KAT Files (36MB) IP Statements Website	Jean-Phillippe Aumasson Guillaume Endignoux	Submit Comment View Comments
Guess Again	Zip File (11MB) KAT Files (42MB) IP Statements Website	Vladimir Shpilrain Mariya Bessonov Alexey Gribov Dima Grigoriev	Submit Comment View Comments
Gui	Zip File (2MB) KAT Files (48MB) IP Statements	Jintai Ding Ming-Shen Chen Albrecht Petzoldt Dieter Schmidt	Submit Comment View Comments

	Website	Bo-Yin Yang	
HILA5	Zip File (1MB) IP Statements Website	Markku-Juhani O. Saarinen	Submit Comment View Comments Round5 *(possible merger of HILA5 & Round 2)*
HiMQ-3	Zip File (1MB) KAT FIles (29MB) IP Statements Website	Kyung-Ah Shim Cheol-Min Park Aeyoung Kim	Submit Comment View Comments
***HK17**	Zip File (2MB) IP Statements Website	Juan Pedro Hecht Jorge Alejandro Kamlofsky	Submit Comment View Comments
HQC	Zip File (11MB) KAT Files (19MB) IP Statements Website	Carlos Aguilar Melchor Nicolas Aragon Slim Bettaieb Loïc Bidoux Olivier Blazy Jean-Christophe Deneuville Philippe Gaborit Edoardo Persichetti Gilles Zémor	Submit Comment View Comments
KCL *(pka OKCN/AKCN/CNKE)*	Zip File (12MB) IP Statements Website	Yunlei Zhao Zhengzhong jin Boru Gong Guangye Sui	Submit Comment View Comments
KINDI	Zip File (12MB) IP Statements Website	Rachid El Bansarkhani	Submit Comment View Comments
LAC	Zip File (8MB) IP Statements Website	Xianhui Lu Yamin Liu Dingding Jia Haiyang Xue Jingnan He Zhenfei Zhang	Submit Comment View Comments
LAKE	Zip File (2MB) IP Statements Website	Nicolas Aragon Olivier Blazy Jean-Christophe Deneuville Philippe Gaborit Adrien Hauteville	Submit Comment View Comments

		Olivier Ruatta Jean-Pierre Tillich Gilles Zemor	
LEDAkem	Zip File (17MB) IP Statements Website	Marco Baldi Alessandro Barenghi Franco Chiaraluce Gerardo Pelosi Paolo Santini	Submit Comment View Comments
LEDApkc	Zip File (21 MB) IP Statements Website	Marco Baldi Alessandro Barenghi Franco Chiaraluce Gerardo Pelosi Paolo Santini	Submit Comment View Comments
Lepton	Zip File (11MB) IP Statements Website	Yu Yu Jiang Zhang	Submit Comment View Comments
LIMA	Zip File (<1MB) KAT Files (54MB) IP Statements Website	Nigel P. Smart Martin R. Albrecht Yehuda Lindell Emmanuela Orsini Valery Osheter Kenny Paterson Guy Peer	Submit Comment View Comments
Lizard	Zip File (1MB) KAT Files (38MB) IP Statements Website	Jung Hee Cheon Sangjoon Park Joohee Lee Duhyeong Kim Yongsoo Song Seungwan Hong Dongwoo Kim Jinsu Kim Seong-Min Hong Aaram Yun Jeongsu Kim Haeryong Park Eunyoung Choi Kimoon kim Jun-Sub Kim Jieun Lee	Submit Comment View Comments
LOCKER	Zip File (7MB) IP Statements Website	Nicolas Aragon Olivier Blazy Jean-Christophe Deneuville Philippe Gaborit Adrien Hauteville Olivier Ruatta Jean-Pierre Tillich	Submit Comment View Comments

		Gilles Zemor	
LOTUS	Zip File (3MB) KAT Files (81MB) IP Statements Website	Le Trieu Phong Takuya Hayashi Yoshinori Aono Shiho Moriai	Submit Comment View Comments
LUOV	Zip File (7MB) KAT Files (97MB) IP Statements Website	Ward Beullens Bart Preneel Alan Szepieniec Frederik Vercauteren	Submit Comment View Comments
McNie	Zip File (11MB) IP Statements Website	Lucky Galvez Jon-Lark Kim Myeong Jae Kim Young-Sik Kim Nari Lee	Submit Comment View Comments
Mersenne-756839	Zip File (2MB) KAT Files (38MB) IP Statements Website	Divesh Aggarwal Antoine Joux Anupam Prakash Mikos Santha	Submit Comment View Comments
MQDSS	Zip File (13MB) IP Statements Website	Simona Samardjiska Ming-Shing Chen Andreas Hulsing Joost Rijneveld Peter Schwabe	Submit Comment View Comments
NewHope	Zip File (7MB) IP Statements Website	Thomas Poppelmann Erdem Alkim Roberto Avanzi Joppe Bos Leo Ducas Antonio de la Piedra Peter Schwabe Douglas Stebila	Submit Comment View Comments
NTRUEncrypt	Zip File (5MB) IP Statements Website	Zhenfei Zhang Cong Chen Jeffrey Hoffstein William Whyte	Submit Comment View Comments
pqNTRUSign	Zip File (5MB) IP Statements Website	Zhenfei Zhang Cong Chen Jeffrey Hoffstein William Whyte	Submit Comment View Comments
NTRU-HRSS-KEM	Zip File (1MB) IP Statements	John M. Schanck Andreas Hulsing	Submit Comment View Comments

	Website	Joost Rijneveld Peter Schwabe	
NTRU Prime	Zip File (1MB) IP Statements Website	Daniel J. Bernstein Chitchanok Chuengsatiansup Tanja Lange Christine van Vredendaal	Submit Comment View Comments
NTS-KEM	Zip File (2MB) KAT Files (38MB) IP Statements Website	Martin Albrecht Carlos Cid Kenneth G. Paterson Cen Jung Tjhai Martin Tomlinson	Submit Comment View Comments
Odd Manhattan	Zip File (1MB) IP Statements Website	Thomas Plantard	Submit Comment View Comments
Ouroboros-R	Zip File (5MB) IP Statements Website	Carlos Aguilar Melchor Nicolas Aragon Slim Bettaieb Loic Bidoux Olivier Blazy Jean-Christophe Deneuville Phillipe Gaborit Adrien Hauteville Gilles Zemor	Submit Comment View Comments
Picnic	Zip File (19MB) KAT Files (71MB) IP Statements Website	Greg Zaverucha Melissa Chase David Derler Steven Goldfeder Claudio Orlandi Sebastian Ramacher Christian Rechberger Daniel Slamanig	Submit Comment View Comments
Post-quantum RSA-Encryption	Zip File (4MB) IP Statements Website	Daniel J. Bernstein Josh Fried Nadia Heninger Paul Lou Luke Valenta	Submit Comment View Comments
Post-quantum RSA-Signature	Zip File (2MB) IP Statements Website	Daniel J. Bernstein Josh Fried Nadia Heninger Paul Lou Luke Valenta	Submit Comment View Comments
pqsigRM	Zip File (<1MB)	Wijik Lee	Submit Comment

	KAT Files (15MB) IP Statements Website	Young-Sik Kim Yong-Woo Lee Jong-Seon No	View Comments
QC-MDPC KEM	Zip File (2MB) IP Statements Website	Atsushi Yamada Edward Eaton Kassem Kalach Philip Lafrance Alex Parent	Submit Comment View Comments
qTESLA	Zip File (7MB) IP Statements Website	Nina Bindel Sedat Akleylek Erdem Alkim Paulo S. L. M. Barreto Johannes Buchmann Edward Eaton Gus Gutoski Juliane Kramer Patrick Longa Harun Polat Jefferson E. Ricardini Gustavo Zanon	Submit Comment View Comments
RaCoSS	Zip File (<1MB) IP Statements Website	Kazuhide Fukushima Partha Sarathi Roy Rui Xu Shinsaku Kiyomoto Kirill Morozov Tsuyoshi Takagi	Submit Comment View Comments
Rainbow	Zip File (1MB) KAT Files (80MB) IP Statements Website	Jintai Ding Ming-Shing Chen Albrecht Petzoldt Dieter Schmidt Bo-Yin Yang	Submit Comment View Comments
Ramstake	Zip File (28MB) IP Statements Website	Alan Szepieniec	Submit Comment View Comments
***RankSign**	Zip File (8MB) KAT Files (57MB) IP Statements Website	Nicolas Aragon Phillipe Gaborit Adrien Hauteviллle Olivier Ruatta Gilles Zemor	Submit Comment View Comments
RLCE-KEM	Zip File (1MB) KAT	Yongge Wang	Submit Comment View Comments

	Files (81MB) IP Statements Website		
Round2	Zip File (31MB) KAT Files (52MB) IP Statements Website	Oscar Garcia-Morchon Zhenfei Zhang Sauvik Bhattacharya Ronald Rietman Ludo Tolhuizen Jose-Luis Torre-Arce Hayo Baan	Submit Comment View Comments Round5 *(possible merger of HILA5 & Round 2)*
RQC	Zip File (8MB) IP Statements Website	Carlos Aguilar Melchor Nicolas Aragon Slim Bettaieb Loic Bidoux Olivier Blazy Jean-Christophe Deneuville Phillippe Gaborit Gilles Zemor	Submit Comment View Comments
***RVB**	Zip File (5MB) IP Statements Website	C. B. Roellgen G. Brands	Submit Comment View Comments
SABER	Zip File (2MB) IP Statements Website	Jan-Pieter D'Anvers Angshuman Karmakar Sujoy Sinha Roy Frederik Vercauteren	Submit Comment View Comments
SIKE	Zip File (2MB) IP Statements Website	David Jao Reza Azarderakhsh Matthew Campagna Craig Costello Luca De Feo Basil Hess Amir Jalali Brian Koziel Brian LaMacchia Patrick Longa Michael Naehrig Joost Renes Vladimir Soukharev	Submit Comment View Comments

		David Urbanik	
SPHINCS+	Zip File (2MB) KAT Files (61MB) IP Statements Website	Andreas Hulsing Daniel J. Bernstein Christoph Dobraunig Maria Eichlseder Scott Fluhrer Stefan-Lukas Gazdag Panos Kampanakis Stefan Kolbl Tanja Lange Martin M Lauridsen Florian Mendel Ruben Niederhagen Christian Rechberger Joost Rijneveld Peter Schwabe	Submit Comment View Comments
***SRTPI**	Zip File (2MB) KAT Files (100MB) IP Statements Website	Yossi (Joseph) Peretz Nerya Granot	Submit Comment View Comments
Three Bears	Zip File (3MB) IP Statements Website	Mike Hamburg	Submit Comment View Comments
Titanium	Zip File (3MB) KAT Files (34MB) IP Statements Website	Ron Steinfeld Amin Sakzad Raymond K. Zhao	Submit Comment View Comments
WalnutDSA	Zip File (9MB) IP Statements Website	Derek Atkins Iris Anshel Dorian Goldfeld Paul E Gunnells	Submit Comment View Comments

*** denotes algorithm has been withdrawn**

Post-Quantum Cryptography StandardizationCall for ProposalsExample FilesRound 1 SubmissionsWorkshops and TimelineContact InfoEmail List (PQC Forum)PQC Archive

Created January 03, 2017, Updated September 04, 2018