

ITASEC18

ITALIAN CONFERENCE ON CYBERSECURITY

Milan, 6-9 February 2018



POLITECNICO
MILANO 1863



cini
Cybersecurity
National Lab

Overview of the NIST Post-Quantum Standardization Initiative

Franco Chiaraluce

Università Politecnica delle Marche,
Ancona, Italy
f.chiaraluce@univpm.it



The NIST Post-Quantum Standardization Initiative

- **NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms.**

Rationale:

- ✓ In recent years, there has been a substantial amount of research on quantum computers.
- ✓ If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use.
- ✓ This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere.
- ✓ The goal of *post-quantum cryptography* is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

The NIST Post-Quantum Standardization Initiative (ctd.)

Rationale:

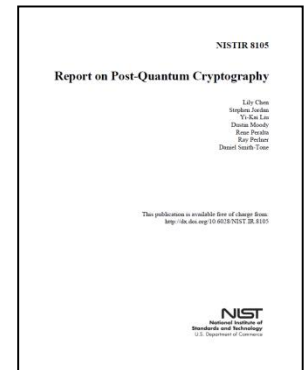
- ✓ The question of when a large-scale quantum computer will be built is a complicated one.
- ✓ Some engineers predict that, within the next twenty or so years, sufficiently large quantum computers will be built to break essentially all public key schemes currently in use.
- ✓ Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure.
- ✓ Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

NIST initiatives


- **April 2-3, 2015** - Workshop on Cybersecurity in a Post-Quantum World, NIST, Gaithersburg, MD

Timeline:

- **Feb. 24-26, 2016** - NIST Presentation at PQCrypto 2016: Announcement and outline of NIST's Call for Submissions, Dustin Moody
- **April 28, 2016** - NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
- **Dec. 20, 2016** - Formal Call for Proposals
- **Nov. 30, 2017** - Deadline for submissions
- **Dec. 4, 2017** - NIST Presentation at AsiaCrypt 2017: The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition", Dustin Moody



NIST Call (Dec. 20, 2016)

 National Institute of Standards and Technology
Information Technology Laboratory

SEARCH: Search

CONTACT SITE MAP

Computer Security Division
Computer Security Resource Center

CSRC Home About Projects / Research Publications News & Events

CSRC HOME > GROUPS > CT > POST-QUANTUM CRYPTOGRAPHY PROJECT

POST-QUANTUM CRYPTO STANDARDIZATION

Call For Proposals Announcement


The National Institute of Standards and Technology (NIST) has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Currently, public-key cryptographic algorithms are specified in [FIPS 186-4, Digital Signature Standard](#), as well as special publications [SP 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography](#) and [SP 800-56B Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography](#). However, these algorithms are vulnerable to attacks from large-scale quantum computers (see [NISTIR 8105 Report on Post Quantum Cryptography](#)). It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

As a first step in this process, NIST [solicited public comment](#) on draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms. The comments received are posted at <http://www.nist.gov/pqcrypto>, along with a summary of the changes made as a result of these comments.

The final submission requirements and the minimum acceptability requirements of a complete and proper candidate algorithm submission, as well as the evaluation criteria that will be used to appraise the candidate algorithms, can be found at <http://www.nist.gov/pqcrypto>. Nominations for post-quantum candidate algorithms may now be submitted, up until the **final deadline of November 30, 2017**. Complete instructions on how to submit a candidate package are posted at <http://www.nist.gov/pqcrypto>.

Appreciation


NIST extends its appreciation to all submitters and those providing public comments during the post-quantum algorithm evaluation process.

 [Call for Proposals](#)

Post-Quantum Cryptography Project
Documents
Workshops / Timeline
Federal Register Notices
Email Listserv
PQC Project Contact
Archive Information

Post-Quantum Cryptography Standardization
[Call for Proposals Announcement](#)
[Call for Proposals](#)
[Submission Requirements](#)
[Minimum Acceptability Requirements](#)
[Evaluation Criteria](#)
[Evaluation Process](#)
[Example Files](#)
[RFC on Submission Requirements and Evaluation Criteria & Public Comments \(Aug 2016\)](#)

[FAQs](#)

 CSRC Webmaster, [Disclaimer Notice](#) & [Privacy Policy](#)
NIST is an Agency of the U.S. Department of Commerce

Last updated: December 19, 2016
Page created: February 29, 2016

Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process

Table of Contents

1. Background
2. Requirements for Submission Packages
 - 2.A Cover Sheet
 - 2.B Algorithm Specifications and Supporting Documentation
 - 2.C Digital and Optical Media
 - 2.D Intellectual Property Statements / Agreements / Disclosures
 - 2.E General Submission Requirements
 - 2.F Technical Contacts and Additional Information
3. Minimum Acceptability Requirements
4. Evaluation Criteria
 - 4.A Security
 - 4.B Cost
 - 4.C Algorithm and Implementation Characteristics
5. Plans for the Evaluation Process
 - 5.A Overview
 - 5.B Technical Evaluation
 - 5.C Initial Planning for the first Post-Quantum Cryptography Standardization Conference

Authority: This work is being initiated pursuant to NIST's responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

1. Background

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will compromise the security of many commonly used cryptographic algorithms.

In particular, quantum computers would completely break many public-key cryptosystems, including RSA, DSA, and elliptic curve cryptosystems. These cryptosystems are used to implement digital signatures and key establishment and play a crucial role in ensuring the confidentiality and authenticity of communications on the Internet and other networks.

Due to this concern, many researchers have begun to investigate *post-quantum* cryptography (PQC) (also called *quantum-resistant* or *quantum-safe* cryptography). The goal of this research is to develop cryptographic algorithms that would be secure against both quantum and classical computers. These algorithms could serve as replacements for

NIST Call: Functionalities (1/3)

- **Public-key encryption:** shall include algorithms for key generation, encryption, and decryption.
- The key generation algorithm shall generate public and private keys, such that messages or symmetric keys encrypted with the public key are recoverable with high probability by decryption with the corresponding private key. If decryption failure is a possibility, it shall occur at a rate consistent with claims made by the submitter.
- At a minimum, the scheme shall support the encryption and decryption of messages that contain symmetric keys of length at least 256 bits.

NIST Call: Functionalities (2/3)

- **Key encapsulation mechanism (KEM):** shall include algorithms for key generation, encapsulation, and decapsulation.
- The key generation algorithm shall generate public and private key pairs, such that encapsulation with the public key and decapsulation with the private key produce the same shared secret, when the encapsulated ciphertext is given as an input to the decapsulate function. If decapsulation failure is a possibility, it shall occur at a rate consistent with claims made by the submitter.
- At a minimum, the KEM functionality shall support the establishment of shared keys of length at least 256 bits.

NIST Call: Functionalities (3/3)

- **Digital signature:** shall include algorithms for key generation, signature generation and signature verification.
- The key generation algorithm shall generate public and private keys, such that a message signed with the private key will be successfully verified with the corresponding public key.
- The scheme shall be capable of supporting a message size up to 2^{63} bits.

Minimum acceptability requirements

1. The algorithms shall be **publicly disclosed** and made available for public review and the evaluation process, and for standardization if selected, freely (i.e., shall be dedicated to the public), or shall be made available in accordance with the rules fixed in other parts of the call.
2. The algorithms shall **not** incorporate major components that are believed to be **insecure** against quantum computers.
3. The algorithms shall provide at least one of the following **functionalities**: public-key encryption, key exchange, or digital signature.
4. The submission package shall provide **concrete values** for any parameters and settings required to achieve the claimed security properties (to the best of the submitter's knowledge).

Evaluation criteria: Security

- **Applications of Public-Key Cryptography**
- **Security Definition for Encryption/Key-Establishment**

“Semantically secure” encryption or key encapsulation with respect to adaptive chosen ciphertext attack (*IND-CCA2 security*), for general use. For estimating security strengths, it may be assumed that the attacker has access to the decryptions of no more than 2^{64} chosen ciphertexts.
- **Security Definition for Ephemeral-Only Encryption/Key-Establishment**

“Semantic security” with respect to chosen plaintext attack (*IND-CPA security*).
- **Security Definition for Digital Signatures**

“Existentially unforgeable” digital signatures with respect to an adaptive chosen message attack (*EUFCMA security*). For estimating security strengths, it may be assumed that the attacker has access to signatures for no more than 2^{64} chosen messages.

Security strength categories

- NIST has defined a separate category for each of the following security requirements (listed in order of increasing strength):

Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for:

- 1) key search on a block cipher with a 128-bit key (e.g. AES128)
- 2) collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256)
- 3) key search on a block cipher with a 192-bit key (e.g. AES192)
- 4) collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384)
- 5) key search on a block cipher with a 256-bit key (e.g. AES 256)

Complexity of quantum attacks

AES 128	2^{170} /MAXDEPTH quantum gates or 2^{143} classical gates
SHA3-256	2^{146} classical gates
AES 192	2^{233} /MAXDEPTH quantum gates or 2^{207} classical gates
SHA3-384	2^{210} classical gates
AES 256	2^{298} /MAXDEPTH quantum gates or 2^{272} classical gates
SHA3-512	2^{274} classical gates

MAXDEPTH (logical gates) = $2^{40} \rightarrow 2^{64} \rightarrow 2^{96}$

Additional security properties

- **Perfect forward secrecy**
- **Resistance to side-channel attacks**
- **Resistance to multi-key attacks**
- **Resistance to misuse**

Cost

Schemes will be evaluated based on:

- **Public key, ciphertext, and signature size**
- **Computational efficiency of public and private key operations**
- **Computational efficiency of key generation**
- **Decryption failures**

Algorithm and implementation characteristics

- **Flexibility**
- **Simplicity**
- **Potential widespread adoption**

Overall submissions

FINAL SUBMISSIONS RECEIVED

- The deadline is past – no more submissions
- 82 total submissions received
 - 23 signature schemes
 - 59 Encryption/KEM schemes

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	23	59	82

After submission

1. By Dic. 21, NIST has completed the reviews for all the submissions received by the deadline. The reviews were to check if submissions were "complete and proper", meeting both NIST submission requirements and minimal acceptance criteria. They were NOT a review on the technical merits.
2. All the submission packages which were accepted (69 out of 82) have been made available at: www.nist.gov/pqcrypto.
3. The authors have been invited to attend the 1st NIST Workshop on PQC Standardization (Fort Lauderdale, FL, 11-13 April 2018) to present their algorithms to NIST staff and conference attendees.
4. The algorithms have been publicly disclosed and made available for public review.

Round 1 submissions (1/6)

Algorithm	Submitters
BIG QUAKE	Alain Couvreur, Magali Bardet, Elise Barelli, Olivier Blazy, Rodolfo Canto-Torres, Philippe Gaborit, Ayoub Otmani Nicolas Sendrier, Jean-Pierre Tillich
BIKE	Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneyasu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zemor
CFPKM	O. Chakraborty, J.-C. Faugere, L. Perret
Classic McEliece	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
Compact LWE	Dongxi Liu, Nan Li, Jongkil Kim, Surya Nepal
CRYSTALS-DILITHIUM	Vadim Lyubashevsky, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehle
CRYSTALS-KYBER	Peter Schwabe, Roberto Avanzi, Joppe Bos, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehle
DAGS	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
Ding Key Exchange	Jintai Ding, Tsuyoshi Takagi. Xinwei Gao, Yuntao Wang
DME	Ignacio Luengo, Martin Avendano, Michael Marco
DRS	Thomas Plantard, Arnaud Sipasseuth, Cedric Dumondelle, Willy Susilo

Round 1 submissions (2/6)

Algorithm	Submitters
DualModeMS	J.-C. Faugere, L. Perret, J. Ryckeghem
Edon-K	Danilo Gligoroski, Kristian Gjosteen
EMBLEM and R.EMBLEM	Minhye Seo, Jong Hwan Park, Dong Hoon Lee, Suhri Kim, Seung-Joon Lee
FALCON	Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang
FrodoKEM	Michael Naehrig, Erdem Alkim, Joppe Bos, Leo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, Douglas Stebila
GeMSS	A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem
Giophantus	Koichiro Akiyama, Yasuhiro Goto, Shinya Okumura, Tsuyoshi Takagi, Koji Nuida, Goichiro Hanaoka, Hideo Shimizu, Yasuhiko Ikematsu
Gravity-SPHINCS	Jean-Phillippe Aumasson, Guillaume Endignoux
Guess Again	Vladimir Shpilrain, Mariya Bessonov, Alexey Gribov, Dima Grigoriev
Gui	Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang
HILA5	Markku-Juhani O. Saarinen
HiMQ-3	Kyung-Ah Shim, Cheol-Min Park, Aeyoung Kim
HK17	Juan Pedro Hecht, Jorge Alejandro Kamlofsky

Round 1 submissions (3/6)

Algorithm	Submitters
HQC	Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor
KINDI	Rachid El Bansarkhani
LAC	Xianhui Lu, Yamin Liu, Dingding Jia, Haiyang Xue, Jingnan He, Zhenfei Zhang
LAKE	Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zemor
LEDAkem	Marco Baldi, Alessandro Barengi, Franco Chiaraluce, Gerardo Pelosi, Paolo Santini
LEDApkc	Marco Baldi, Alessandro Barengi, Franco Chiaraluce, Gerardo Pelosi, Paolo Santini
Lepton	Yu Yu, Jiang Zhang
LIMA	Nigel P. Smart, Martin R. Albrecht, Yehuda Lindell, Emmanuela Orsini, Valery Osheter, Kenny Paterson, Guy Peer
Lizard	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
LOCKER	Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zemor
LOTUS	Le Trieu Phong, Takuya Hayashi, Yoshinori Aono, Shiho Moriai
LUOV	Ward Beullens, Bart Preneel, Alan Szepeieniec, Frederik Vercauteren
McNie	Lucky Galvez, Jon-Lark Kim, Myeong Jae Kim, Young-Sik Kim, Nari Lee

Round 1 submissions (4/6)

Algorithm	Submitters
Mersenne-756839	Divesh Aggarwal, Antoine Joux, Anupam Prakash, Mikos Santha
MQDSS	Simona Samardjiska, Ming-Shing Chen, Andreas Hulsing, Joost Rijneveld, Peter Schwab
NewHope	Thomas Poppelmann, Erdem Alkim, Roberto Avanzi, Joppe Bos, Leo Ducas, Antonio de la Piedra, Peter Schwabe, Douglas Stebila
NTRUEncrypt	Zhenfei Zhang, Cong Chen, Jeffrey Hoffstein, William Whyte
pqNTRUSign	Zhenfei Zhang, Cong Chen, Jeffrey Hoffstein, William Whyte
NTRU-HRSS-KEM	John M. Schanck, Andreas Hulsing, Joost Rijneveld, Peter Schwabe
NTRU Prime	Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal
NTS-KEM	Martin Albrecht, Carlos Cid, Kenneth G. Paterson, Cen Jung Tjhai, Martin Tomlinson
Odd Manhattan	Thomas Plantard
OKCN/AKCN/CNKE	Yunlei Zhao, Zhengzhong jin, Boru Gong, Guangye Sui
Ouroboros-R	Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Adrien Hauteville, Gilles Zemor
Picnic	Greg Zaverucha, Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig
Post-quantum RSA-Encryption	Daniel J. Bernstein, Josh Fried, Nadia Heninger, Paul Lou, Luke Valenta
Post-quantum RSA-Signature	Daniel J. Bernstein, Josh Fried, Nadia Heninger, Paul Lou, Luke Valenta

Round 1 submissions (5/6)

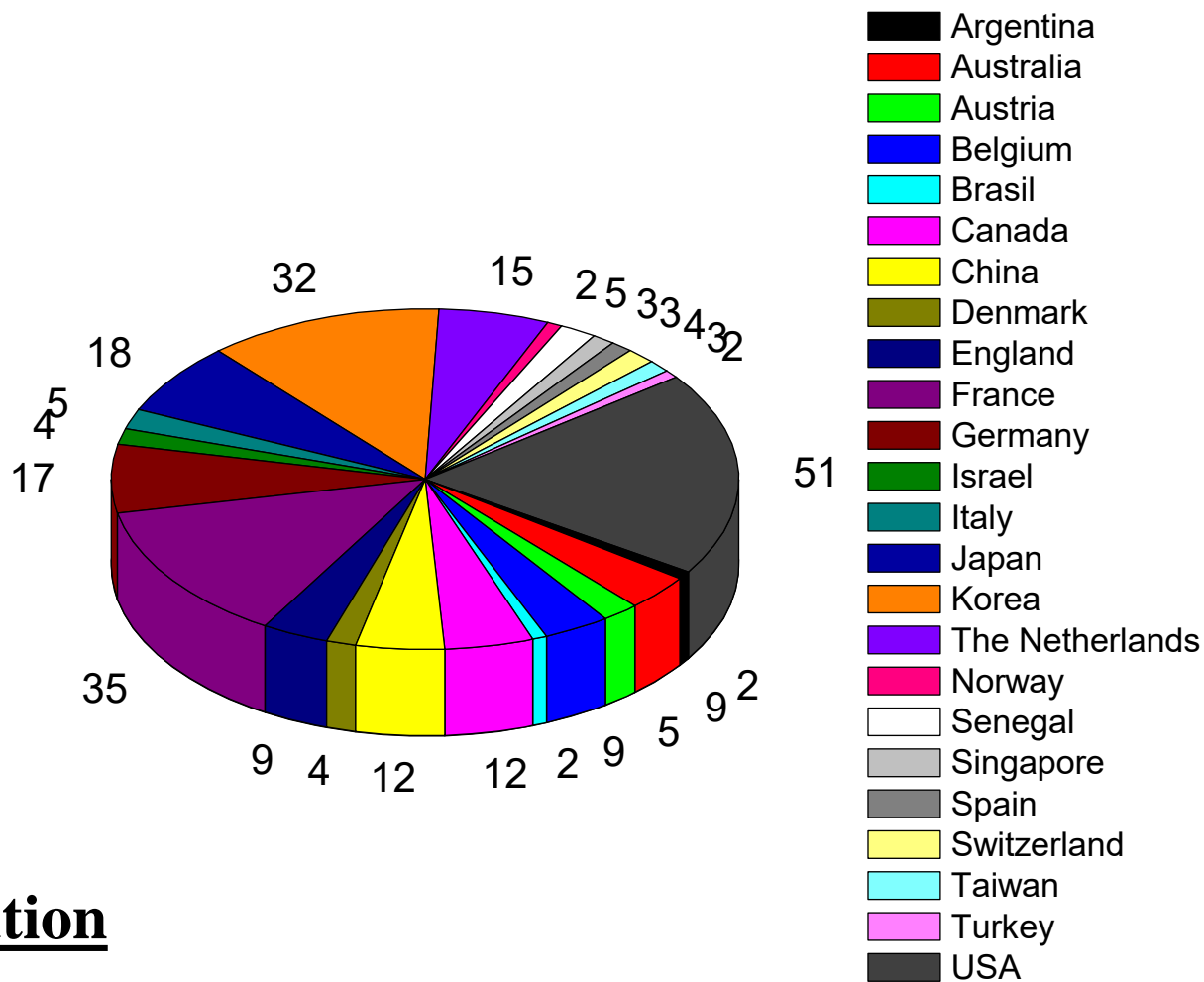
Algorithm	Submitters
pqsigRM	Wijik Lee, Young-Sik Kim, Yong-Woo Lee, Jong-Seon No
QC-MDPC KEM	Atsushi Yamada, Edward Eaton, Kassem Kalach, Philip Lafrance, Alex Parent
qTESLA	Nina Bindel, Sedat Akleylek, Erdem Alkim, Paulo S. L. M. Barreto, Johannes Buchmann, Edward Eaton, Gus Gutoski, Juliane Kramer, Patrick Longa, Harun Polat, Jefferson E. Ricardini, Gustavo Zanon
RaCoSS	Kazuhide Fukushima, Partha Sarathi Roy, Rui Xu, Shinsaku Kiyomoto, Kirill Morozov, Tsuyoshi Takagi
Rainbow	Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang
Ramstake	Alan Szeplieniec
RankSign	Nicolas Aragon, Phillipe Gaborit, Adrien Hauteville, Olivier Ruatta, Gilles Zemor
RLCE-KEM	Yongge Wang
Round2	Oscar Garcia-Morchon, Zhenfei Zhang, Sauvik Bhattacharya, Ronald Rietman, Ludo Tolhuizen, Jose-Luis Torre-Arce
RQC	Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillippe Gaborit, Gilles Zemor
RVB	C. B. Roellgen, G. Brands
SABER	Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, Frederik Vercauteren
SIKE	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, David Urbanik

Round 1 submissions (6/6)

Algorithm	Submitters
SPHINCS+	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
SRTPI	Yossi (Joseph) Peretz, Nerya Granot
Three Bears	Mike Hamburg
Titanium	Ron Steinfeld, Amin Sakzad, Raymond K. Zhao
WalnutDSA	Derek Atkins, Iris Anshel, Dorian Goldfeld, Paul E Gunnells

Submitters summary

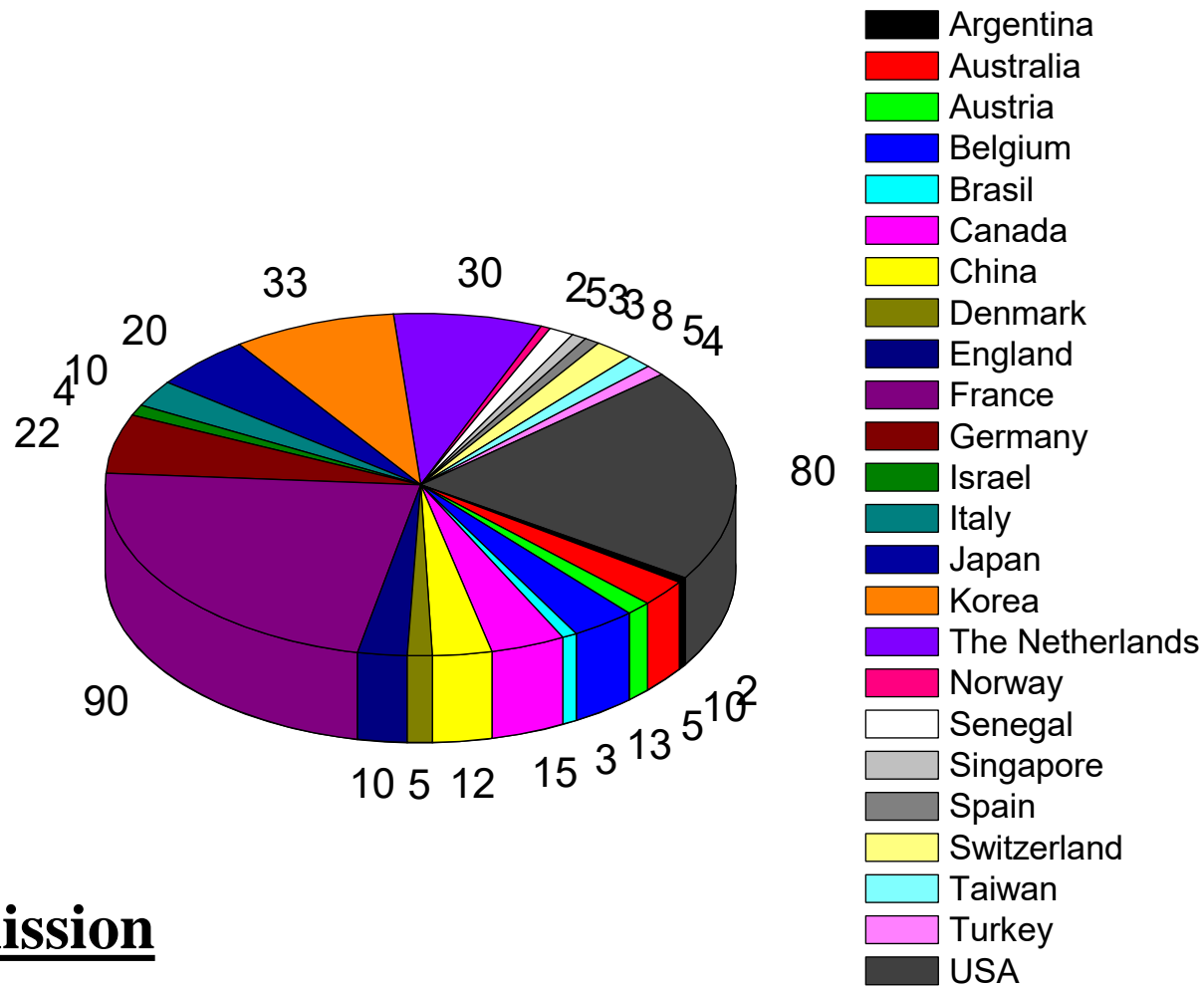
263 researchers involved



By institution

Submitters summary (ctd.)

394 authorships involved



Comments

← → ↻ 🏠 <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions> 🔍 Cerca

⚙️ Più visitati 📺 Come iniziare [History of Updates](#)

Algorithm Information
KAT files are included in zip file unless they were too large

Algorithm		Submitters	Comments
BIG QUAKE	Zip File (4MB) 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) Website	Nicolas Aragon Paulo Barreto Slim Bettaieb Loic Bidoux Olivier Blazy Jean-Christophe Deneuville Phillipe Gaborit Shay Gueron Tim Guneyso Carlos Aguilar Melchor Rafael Misoczki Edoardo Persichetti	Submit Comment View Comments

Contact Info
[Email List \(PQC Forum\)](#)
[PQC Archive](#)

CONTACTS

PQC Crypto Technical Inquiries
pqc-comments@nist.gov

Dr. Lily Chen
301-975-6974

Dr. Dustin Moody
301-975-8136

Dr. Yi-Kai Liu
301-975-6499

GROUP

[Cryptographic Technology](#)

TOPICS

Security and Privacy: [post-quantum cryptography](#),

RELATED PROJECTS

pqc-forum@list.nist.gov

Posted official comments: **151** (@ 7/2/18)

Comments (Ex.)

Da: D. J. Bernstein <djb@cr.yp.to>

Inviato: lunedì 25 dicembre 2017 18:15

A: pqc-forum@list.nist.gov

Cc: pqc-comments@nist.gov

Oggetto: [pqc-forum] OFFICIAL COMMENT: HK17

Dear designers, dear all,

The following attack script breaks HK17 for all proposed parameters.

Specifically, this script breaks the Python key-exchange implementation included in the HK17 submission. This key-exchange implementation appears to match the intent of the HK17 documentation, except that the documentation includes a normalization step; this step does not affect the attack.

This attack takes $p+1$ simple computations (and is a search so Grover's algorithm is applicable, but all proposed parameters are small enough to be broken by a non-quantum attack). For comparison, the submission says

- * 2^{64} pre-quantum security for $p=251$,
- * 2^{128} pre-quantum security for $p=65521$,
- * 2^{256} pre-quantum security for $p=4294967291$, and
- * 2^{512} pre-quantum security for $p=18446744073709551557$.

Our attack takes about 2^8 , 2^{16} , 2^{32} , and 2^{64} simple computations for these parameter sets.

Da: Lorenz Panny <l.s.panny@tue.nl>

Inviato: lunedì 25 dicembre 2017 11:03

A: pqc-comments@nist.gov

Cc: pqc-forum@list.nist.gov

Oggetto: [pqc-forum] OFFICIAL COMMENT: RVB

Dear all,

the following sage script quickly computes the secret key from a given public key in the RVB submission:

<https://yx7.cc/files/chaos.sage.txt>

The attack is essentially the algorithm of [0] except for using LLL to find k such that $a+kb$ is close to an integer. The script successfully recovers the secret keys of all known-answer tests.

-- Lorenz

[0] <https://arxiv.org/abs/cs/0411030>

- After three to five years (NIST estimate) some algorithms could be selected for standardization.
- However, due to developments in the field, this could change.





Thanks for
your attention.