From: Dang, Quynh (Fed)
To: Moody, Dustin (Fed)
Subject: Re: 1st Round Report
Date: Monday, December 10, 2018 2:45:49 PM
Attachments: PQC Report on Round 1_NISTIR update1.docx

Hi Dustin,

See my proposed changes in the NTRU and NTRU Prime sections.

One more thing: you skipped the sentence about security property of being a large Galois group. It seems to me that Mike Hamburg kinda implicitly agreed that being a large Galois group might have security benefit.

If an attack is based on the Galois group (all of the automorphisms), a large Galois group would be computationally expensive to be computed. For the size of 4500!, it is around 10^14,5000.

Quynh.

From: Moody, Dustin (Fed)
Sent: Monday, December 10, 2018 1:36:42 PM
To: Alagic, Gorjan (Assoc); Alperin-Sheriff, Jacob (Fed); Apon, Daniel C. (Fed); Cooper, David A. (Fed); Dang, Quynh (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Perlner, Ray (Fed); Robinson, Angela Y. (Fed); Smith-Tone, Daniel (Fed); (b) (6)
Subject: 1st Round Report

I did a revision on some of the write-ups to make them more uniform. I think we want to try and make sure they are all written about the same level of detail, and include the important characteristics, strengths, and weaknesses. Please take a look and let me know of any suggested revisions. I put some comments in a few places where I thought changes might be good.

Thanks,

Dustin

NISTIR 8240

Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process

First Author
Second Author
Etc.

Commented [MD(1]: Split into authors and team members:
Dustin Moody
Lily Chen
Ray Perlner
Jacob Alperin-Sheriff
Carl Miller
Gorjan Alagic
Yi-Kai Liu
Daniel Smith-Tone
Quynh Dang
Sara Kerman
David Cooper
Daniel Apon
Bill Fefferman?
Larry Bassham
Morrie Dworkin
John Kelsey
Angela Robinson
Rene Peralta
Andrew Regenscheid

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8240

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8240

Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process

First Author
Second Author, etc.
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8240

January 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Internal Report 8240
16 pages (January 2019)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8240

Commented [FJ(2]: This is a DocProperty Field ("Pages") that automatically inserts the total number of document pages. Right-click and select "Update Field" to update value.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: pqc-comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

The National Institute of Standards and Technology is in the process of selecting one or more public-key cryptographic algorithms through a public competition-like process. The new public-key cryptography standards will specify one or more additional digital signature, public-key encryption, and key-establishment algorithms to augment FIPS 186-4, Digital Signature Standard (DSS), 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, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization. It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers.

In November 2017, 82 candidate algorithms were submitted to NIST for consideration. Among these, 69 met both the minimum acceptance criteria and our submission requirements, and were accepted as First-Round Candidates on Dec. 20, 2017, marking the beginning of the First Round of the NIST Post-Quantum Cryptography Standardization Process. This report describes the evaluation criteria and selection process, based on public feedback and internal review of the first-round candidates, and summarizes the 26 candidate algorithms announced on January 7, 2019 for moving forward to the second round of the competition. The 17 Second-Round Candidate public-key encryption and key-establishment algorithms are BIKE, Classic McEliece, CRYSTALS-KYBER, FrodoKEM, HQC, LAC, LEDAcrypt (merger of LEDAkem/LEDApkc), NewHope, NTRU (merger of NTRUEncrypt/NTRU-HRSS-KEM), NTRU Prime, NTS-KEM, ROLLO (merger of LAKE/LOCKER/Ouroboros-R), Round5 (merger of Hila5/Round2), RQC, SABER, SIKE, and Three Bears. The 9 Second Round Candidates for digital signatures are CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow, and SPHINCS+.

Commented [MD(3]: If date changes, replace all instances of January 7rd

Keywords

cryptography; digital signatures; post-quantum cryptography; public-key encryption; key-establishment mechanism (KEM), quantum resistant; quantum safe

Commented [MD(4]: Any other keywords?

Supplemental Content

The NIST Post-Quantum Cryptography Standardization Process webpage is available at:

https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

Acknowledgments

NIST is grateful for the efforts of all candidate submission teams, who developed, designed, and analyzed post-quantum public-key algorithms and prepared detailed submission packages describing their algorithms. The cryptographic community's response of 82 candidate algorithms submitted to the competition was very encouraging. We were also pleased about the graceful and forthright manner with which several of the submitters recognized and accepted the shortcomings of their submissions.

NIST is also grateful for the efforts of those in the cryptographic community that provided security, implementation and performance analysis of the candidate algorithms during the first round, as well as the numerous cryptanalysts that attacked many of the submissions. NIST would not be able to select new post-quantum public-key algorithm for standardization without the combined efforts of these individuals and the algorithm submitters.

The authors of this report are also appreciative of the efforts by the other members of NIST's PQC team, who reviewed candidate algorithms, analysis and public comments; performed testing; provided technical and administrative support; and participated in numerous meetings to discuss the selection of the first-round candidates. They are: (list the rest of the team members here).

Commented [MD(5]: Fill in with the appropriate names:
Dustin Moody
Lily Chen
Ray Perlner
Jacob Alperin-Sheriff
Carl Miller
Gorjan Alagic
Yi-Kai Liu
Daniel Smith-Tone
Quynh Dang
Sara Kerman
David Cooper
Daniel Apon
Bill Fefferman
Larry Bassham
Morrie Dworkin
John Kelsey
Angela Robinson
Rene Peralta
Andrew Regenscheid

Table of Contents

Commented [MD(6]: Get header fixed so shows 8420 in automatic way

List of Appendices

1 Introduction

The National Institute of Standards and Technology is in the process of selecting one or more public-key cryptographic algorithms through a public competition-like process. The new public-key cryptography standards will specify one or more additional digital signature, public-key encryption, and key-establishment algorithms to augment FIPS 186-4, Digital Signature Standard (DSS) [1], as well as special publications SP 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography [2], and SP 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization [3]. It is intended that these algorithms will be capable of protecting sensitive U.S. government information well into the foreseeable future, including after the advent of quantum computers. The competition-like process will be referred to as the NIST PQC Standardization Process hereafter in this document.

The PQC standardization process is NIST's response to advances in the development of quantum computers. These machines 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 be able to break the public-key cryptosystems currently standardized by NIST, which consist of digital signatures and key-establishment schemes. Quantum computers will have an impact on symmetric-key cryptosystems, however the impact will not be as drastic. The goal of post-quantum cryptography (PQC) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing protocols and networks.

Prior to beginning the NIST PQC Standardization Process, NIST held a workshop in April 2015 [4] to discuss issues related to post-quantum cryptography and its potential future standardization. One year later, NIST released NISTIR 8105, Report on Post-Quantum Cryptography [5], which shared NIST's understanding about the status of quantum computing and post-quantum cryptography and outlined NIST's initial plan to move forward in that space. The preliminary details of the NIST PQC Standardization Process were announced in a presentation [6] at PQCrypto 2016.

NIST published Proposed Requirements and Evaluation Criteria in a Federal Register Notice in August 2016 [7] for public comment. These requirements and evaluation criteria were updated, based on public feedback, and included in a later, second Federal Register Notice published on December 20, 2016 (FRN-Dec16) [8]. This Notice called for public submissions for post-quantum public-key cryptographic algorithms and marked the start of the NIST PQC Standardization Process.

Candidate submissions were due on November 30, 2017, at which time NIST received 82 submission packages. This was a great response from the worldwide cryptographic community, which had submitted 21 candidate algorithms for the AES competition in 1998 [9], and 64 packages for the SHA-3 competition in 2008 [10]. Of the 82 submissions, NIST announced the acceptance of 69 First-Round Candidates as meeting both the submission requirements and minimum acceptability criteria on December 20, 2017. The 69 submissions consisted of 19 digital signature schemes, and 45 public-key encryption (PKE) or key

encapsulation mechanisms (KEMs). Submission packages of the first-round candidates were posted online at www.nist.gov/pqcrypto for public review and comment.

NIST held the First NIST PQC Standardization Process Conference in Ft. Lauderdale, FL on April 11-13, 2018 [11], co-located with PQCrypto 2018. Submitters of the accepted first-round candidates were invited to present their algorithms. NIST also discussed their plan to narrow down the first-round candidates to a more manageable number for further studies by the summer of 2019 and start the second-round of the Standardization Process. Throughout the first round, NIST received much feedback from the cryptographic community. Based on the public feedback and internal reviews of the first-round candidates, NIST announced the selection of 26 algorithms as Second-Round Candidates on January 7, 2019 to move forward to the next stage of the standardization process.

Below is a timeline of major events with respect to the NIST PQC Standardization Process.

- April 2-3, 2015 Workshop on Cybersecurity in a Post-Quantum World, NIST, Gaithersburg, MD
- February 24, 2016 PQC Standardization: Announcement and outline of NIST's Call for Submissions presentation given at PQCrypto 2016
- April 28, 2016 NISTIR 8105, Report on Post-Quantum Cryptography, released
- August 2, 2016 Federal Register Notice - Proposed Requirements and Evaluation Criteria announced for public comment
- December 20, 2016 Federal Register Notice – Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms
- November 30, 2017 Submission Deadline for NIST PQC Standardization Process
- December 20, 2017 First-Round Candidates were announced. The public comment period on the first-round candidates began.
- April 11-13, 2018 First NIST PQC Standardization Conference, Ft. Lauderdale, FL
- January 7, 2019 The First Round ended and the Second Round began. Second-Round candidates announced. The public comment period on the second-round candidates began.
- March 15, 2019 Deadline for updated submission packages for the Second Round
- August 22-24, 2019 2nd NIST PQC Standardization Conference, Santa Barbara, CA

1.1 Purpose and Organization of this Document

The purpose of this document is to report on the **first round** of the NIST PQC Standardization Process and is organized as follows.

Section 2 describes the determination of the first-round candidates using the submission requirements and minimum acceptability requirements defined in FRN-Dec16 [8] for all submissions. It then describes the evaluation criteria and selection process used to ultimately select the second-round candidates.

Section 3 summarizes the 26 selected second-round candidates. For each candidate, we provide a brief description of the algorithm and the properties of the algorithm that interested us, as well as characteristics that might cause some concern. This report focuses on the reasons why candidate algorithms were selected, rather than providing detailed justifications for why candidate algorithms were not selected to move to the next round.

Section 4 describes the next steps in the NIST PQC Standardization Process, including provisions for allowable modifications to the second-round candidates and the evaluation process for selecting finalists.

2 Evaluation Criteria and the Selection Process

2.1 Acceptance of the First Round Candidates

NIST received 82 candidate algorithm submission packages by the November 30, 2017 entry deadline for the NIST PQC Standardization Process. Of these, NIST accepted 69 first-round candidates as meeting both the submission requirements and the minimum acceptability criteria for being "complete and proper submissions", as defined in FRN-Dec16. The criteria included provisions for reference and optimized C code implementations, known-answer tests, a written specification, and required intellectual property statements. In addition, the algorithms were required to be implementable in a wide range of hardware and software platforms.

First Round Candidates

BIG QUAKE	Gui	NewHope
BIKE	HILA5	NTRUEncrypt
CFPKM	HiMQ-3	NTRU-HRSS-KEM
Classic McEliece	HK-17	NTRU Prime
Compact LWE	HQC	NTS-KEM
CRYSTALS-DILITHIUM	KCL	Odd Manhattan
CRYSTALS-KYBER	KINDI	Ouroboros-R
DAGS	LAC	Picnic
Ding Key Exchange	LAKE	Post-quantum RSA Encryption
DME	LEDAkem	Post-quantum RSA Signature
DRS	LEDApkc	pqNTRUSign
DualModeMS	Lepton	pqsigRM
Edon-K	LIMA	QC-MDPC-KEM
EMBLEM/R.EMBLEM	Lizard	qTESLA
FALCON	LOCKER	RaCoSS
FrodoKEM	LOTUS	Rainbow
GeMSS	LUOV	Ramstake
Giophantus	McNie	RankSign
Gravity-SPHINCS	Mersenne-756839	RLCE-KEM
Guess Again	MQDSS	Round2

RQC	SIKE	Three Bears
RVB	SPHINCS+	Titanium
SABER	SRTPI	WalnutDSA

These were the sole criteria used to judge the 82 submission packages. Other factors, such as security, cost, and algorithm and implementation characteristics of the candidates did not enter the review process prior to the first round, nor did cryptanalysis or performance data of a submission impact the acceptance of the first-round candidates.

2.2 Evaluation Criteria

FRN-Dec16 identified three broad categories of evaluation criteria that would be used to compare candidate algorithms throughout the NIST PQC Standardization Process. The three categories are: 1) security, 2) cost and performance, and 3) algorithm and implementation characteristics. These categories are described below, along with a discussion of how they impacted the first round candidate evaluations.

2.2.1 Security

As was the case for the past AES and SHA-3 competitions, security is the most important factor when evaluating the candidate post-quantum algorithms. NIST intends to standardize post-quantum public-key algorithms for use in a wide variety of protocols, such as TLS, SSH, IKE, IPsec, and DNSSEC. Schemes will be evaluated by the security they provide in these (and other) applications.

Submitters were encouraged, but not required, to provide proofs of security in relevant models. For general-use encryption and key-establishment schemes, FRN-Dec16 asked for "semantically secure" schemes with respect to adaptive chosen ciphertext attack (IND-CCA2 security). For ephemeral use cases, NIST will consider semantic security with respect to chosen plaintext attack (IND-CPA security). Digital signature schemes need to enable existentially unforgeable signatures with respect to an adaptive chosen message attack (EUF-CMA security).

While recognizing that there are significant uncertainties in estimating the security strengths of the post-quantum candidate algorithms, NIST defined five security categories to be able to better compare the security strength provided by the submissions. Submitters were asked to provide a preliminary classification, according to the definitions provided in FRN-Dec16, with a focus on meeting the requirements for categories 1, 2, and/or 3.

Commented [MD(7]: Do we need to expand on this? Do we need to talk more about quantum security in this paragraph?

NIST also mentioned other desirable security properties, such as perfect forward secrecy, resistance to side-channel and multi-key attacks, and resistance to misuse. In addition, NIST required submission packages to summarize known cryptanalytic attacks on the scheme and complexity estimates for these attacks.

2.2.2 Cost and Performance

FRN-Dec16 identified cost as the second-most important criterion when evaluating candidate

algorithms. In this case, cost includes computational efficiency and memory requirements. This includes, for example:

- The size of public keys, ciphertext, and signatures
- Computation efficiency of key generation, as well as the public and private key operations
- Decryption failures

Computational efficiency essentially refers to the speed of an algorithm. NIST hopes that candidate algorithms would offer comparable or improved performance over the currently standardized public-key algorithms. Memory requirements refer both to code size and random-access memory (RAM) requirements for software implementations, as well as gate counts for hardware implementations.

FRN-Dec16 required all submitters to include performance estimates on the NIST reference platform, an Intel x64 running Windows or Linux and supporting the GCC compiler. NIST performed a preliminary efficiency analysis on the reference platform, but also invited the public to conduct similar tests on additional platforms.

2.2.3 Algorithm and Implementation Characteristics

The NIST PQC Standardization Process received many candidate algorithms with new and interesting designs, and with unique features that are not present in the NIST standardized public-key algorithms. Candidate algorithms with greater flexibility may be given preference over other algorithms. This includes algorithms capable of running efficiently on a wide variety of platforms, as well as algorithms that use parallelism or instruction set extensions to achieve higher performance. In addition, simple and elegant designs are preferable, in order to encourage understanding, analysis and design confidence. Finally, NIST will consider any factors which might hinder or promote adoption of an algorithm or implementation, including, but not limited to, intellectual property covering an algorithm or implementation and the availability and terms of licenses to interested parties.

2.3 Selection of Second Round Candidates

NIST selected 26 second-round candidates from the 69 first-round candidates using the evaluation criteria specified in FRN-Dec16. In relative order of importance, NIST considered the security, cost and performance, and algorithm and implementation characteristics of a candidate in selecting the second-round candidates.

For the security evaluation of an algorithm, NIST studied the security arguments presented in the submission package, as well as external cryptanalysis submitted to NIST or published elsewhere. NIST researchers also conducted internal cryptanalysis.

NIST considered not only attacks that directly demonstrated that a candidate fell short of NIST's stated security targets, but also attacks that brought the candidate's underlying security assumptions into question, or that looked like they had room for improvement. NIST also considered the overall quantity, quality, and maturity of analysis relevant to each candidate, including analysis of similar schemes.

After security, performance was the next most important criterion in selecting the second-round candidates. When evaluating the performance of the candidates, NIST considered the performance and memory estimates given by the submitters in their submission documentation and in their presentations at the First SHA-3 Candidate Conference. NIST also performed internal performance benchmarks using the code from the submission - packages. In addition, NIST considered the external feedback and performance estimates provided by the cryptographic community. We note that NIST stated "performance considerations will not play a major role in the early portion of the evaluation process [12,13]."

In a few cases, a submitted design was selected in part for its uniqueness and elegance. NIST generally favored those designs that were based on clear design principles or otherwise illustrative of an innovative idea. NIST feels that the diversity of designs will provide an opportunity for cryptographers and cryptanalysts to expand the scope of ideas in their field, and it will also be less likely that a single type of attack will eliminate the bulk of the candidates remaining in the competition.

Second Round Candidates

BIKE	LEDAcrypt	Rainbow
Classic McEliece	LUOV	ROLLO
CRYSTALS-DILITHIUM	MQDSS	Round5
CRYSTALS-KYBER	NewHope	RQC
FALCON	NTRU	SABER
FrodoKEM	NTRU Prime	SIKE
GeMSS	NTS-KEM	SPHINCS+
HQC	Picnic	Three Bears
LAC	qTESLA	

3 Summary of Second Round Candidates

Each of the candidates selected to move on the next round is discussed below, including a summary of the basic design, performance characteristics, and known (crypt)analysis. In addition, the discussion includes suggested areas that the submitters may wish to address in order to improve their candidate's chances of making it further in the process.

We first discuss the 17 public-key encryption and key-establishment schemes, and then the 9 digital signature schemes.

3.1 CRYSTALS-KYBER

Kyber is a family of key encapsulation mechanisms offering chosen ciphertext (i.e., IND-CCA) security based on the presumed post-quantum hardness of the Module Learning with Errors (MLWE) problem. At the core of Kyber is a standard Learning with Errors (LWE)-style CPA-secure public-key encryption scheme, where the underlying algebraic object is a module over a power-of-2 cyclotomic ring. This choice of parameters enables very efficient computations using

the Number Theoretic Transform (NTT). The noise is sampled according to a centered binomial distribution. CCA security is achieved via a well-known variant of the Fujisaki-Okamoto transform, where the session key is transported using an encryption-based approach. Kyber offers a straightforward way of adjusting security strength between three settings: one simply varies the rank of the underlying module (in the range {2,3,4}) and adjusts the noise distribution parameter (in the range {5,4,3}, respectively.) In terms of performance, Kyber is among the most competitive proposals for key exchange.

For security, Kyber relies on a variant of a well-studied problem. The submission offers a tight security proof in the random oracle model (ROM) and a non-tight security proof in the quantum random oracle model (QROM), both based on the MLWE assumption. However, a potential issue is that the security proof does not directly apply to Kyber itself, but rather to a modified version of the scheme which does not compress the public key. Without this modification, Kyber may in fact be relying on a different (or additional) rounding-like assumption. If that is the case, this may lead to a cryptanalytic concern, as the known reductions between MLWE and Module Learning with Rounding (MLWR) may not apply for the parameters selected by Kyber.

3.2 FrodoKEM

FrodoKEM is a CCA-secure key encapsulation mechanism that uses algebraically unstructured lattices. The security is based on the standard learning with errors problem. The secrets are sampled from a discrete Gaussian distribution over the integers and the algorithm is implemented in constant time. Extensive analysis has been devoted to the security of LWE for various parametrizations.

FrodoKEM takes a conservative approach resulting in larger key sizes than other lattice schemes. However FrodoKEM still manages to present lower bandwidth and faster running times than other unstructured lattices submissions.

Commented [MD(8]: Do we want to add a bit more about this?

The FrodoKEM specification includes parameter sets for security levels 1 and 3, and may wish to consider providing a parameter set for level 5.

3.3 LAC

LAC is a cryptosystem based on the poly-LWE variant of the Learning With Errors problem. One notable difference from other similar schemes include the use of a modulus q=251, allowing each element of a polynomial to fit in a single byte. For the problem to remain secure with such a small modulus, they use a very narrow distribution for secrets and error, as well as a BCH code to decode to a shared secret.

The scheme is very fast and has rather small public keys and ciphertexts. However, NIST lacks full confidence in the robustness of the scheme under CCA and side-channel attacks, as several public comments have already demonstrated. Second round tweaks will need to address these issues in order for LAC to remain competitive.

3.4 NewHope

NewHope is a lattice-based cryptosystem suite of unauthenticated KEMs, achieving CPA and

CCA security based on the quantum hardness of the Ring Learning with Errors (RLWE) problem. The scheme uses power-of-2 cyclotomic rings with a common modulus. The RLWE secret and error distributions are both the centered binomial distribution, and the public parameter is ephemeral. Polynomial multiplication is specified using the NTT. CCA security is achieved by a variant of the Fujisaki Okamoto transform. The session key is transported using an encryption-based approach for noisy key agreement.

NewHope has competitive performance in terms of bandwidth and clock cycles among the candidates for post-quantum key-establishment. Some candidates at this stage may have superior performance, but in many cases, this is due to more aggressive design choices, which may or may not be preferable in the long-term.

At present, we are aware of no analysis that raises questions about NewHope's security.

Commented [MD(9]: Remove this line?

3.5 NTRU (merger of NTRUEncrypt and NTRU-HRSS-KEM)

NTRU ~~c~~Encryption is a lattice-based public-key encryption scheme which was invented around 1996 [14]. It is a one-way CPA-secure (OW-CPA) public key encryption scheme whose security has been reasonably-well understood and scrutinized for decades. Many variants of the scheme and their derived key encapsulation mechanisms have been developed since, including the NTRU-HRSS-KEM [15] and NTRUEncrypt [16] submissions. These two submissions~~candidates~~ have announced a merged scheme, which will be known as NTRU.

Commented [MOU10]: "NTRUEncrypt" in the first sentence is not the NTRUEncrypt in the submission. So, your revised text was not clear. I modified the text to make it clearer.

[15] and [16] are links to the submissions.

The KEM in the merged submission is a tight IND-CCA2 security transformation from a deterministic OW-CPA-secure public key encryption scheme in the quantum random oracle model. The submission has two options for the deterministic PKE scheme in the KEM. The derived KEM offers perfect correctness (i.e. no legitimate decryption failures) and avoids both the "evaluation at 1" issue and invertibility checks during key generation.

Commented [MD(11]: Do we want to use this term? Also used in NTRUprime

Fine.

Three parameter sets are specified with three ring instances (n being 701, 443 or 743 bits). The KEM has good sizes for keys and ciphertext. Encapsulation and decapsulation seem to be efficient.

Commented [MD(12]: Suggestions for what they need to change/add? Or drawbacks?

There are 2 options that they can consider. The first one is to drop one ring since 701 and 743 are close. The second is to use only 1 encryption scheme. The HRSS option is superior (in my opinion) because variables are taken from uniformly random distributions (no fixed-type restrictions for g and m), but that is a minor thing. NTRU Prime uses fixed-weights, not uniformly random variables either.

The issue is that if we ask them to do that: they would feel agonized because the 2 teams will have to fight hard again. I don't think it would hurt the analysis effort if you leave them as they are.

3.6 NTRU Prime

The NTRU Prime submission includes two distinct KEMs, known as "Streamlined NTRU Prime" and "NTRU LPRime". The KEMs are both CCA-secure built on deterministic OW-CPA-secure public key encryption functions. In Streamlined NTRU Prime, a rounding technique ~~function~~ is used in encapsulation instead of using a message m as in the original NTRU ~~c~~Encryption. ~~from each coefficient of hr gets rounded deterministically to an element in a subset of Z/q instead of Z/q itself which removes the need of the message m.~~ NTRU LPRime can be considered as a ring-learning-with-rounding (RLWR)-based KEM which has only one secret random variable generated in key generation and encapsulation steps and those steps deploy the rounding technique.

Commented [MOU13]: New text.

Commented [MD(14]: Make less technical – more like the description of NTRU LPRime

The main novelty of the candidate is using an irreducible non-cyclotomic polynomial, and an inert prime q so that the relevant ring is actually a field with large Galois group. These design

choices were made to avoid non-trivial ring homomorphisms and the structure of cyclotomic polynomial rings which are potential security weaknesses. In addition, the KEMs have perfect correctness.

The KEMs have good sizes for keys and ciphertexts. Encapsulation and decapsulation speeds seem to be very competitive against other candidates. NTRU LPRime also has fast key generation. The two KEMs use the same ring (field) with two different parameter sets, all with their claimed security level as 5. The NTRU Prime team may wish to consider adding other parameter sets for other security levels.

3.7 Round5 (merger of HILA5 and Round2)

Round5 is a lattice-based cryptosystem over prime cyclotomic rings, formed by a merger between Round2 and Hila5. The scheme proposes a KEM and public-key encryption scheme with security based on the decision "learning with rounding" problem with sparse ternary secrets, including a ring-variant. Error-correcting code XEf is applied to reduce decryption and decapsulation failures. This error-correcting code is a generalized version of XE5, a highlight and original contribution of Hila5. Although XEf is designed to correct an arbitrary number of errors, only 3-bit errors are corrected in the parameter set included in the Round5 documentation.

Round5 offers competitive performance and some of the lowest bandwidth requirements among the lattice-based proposals. The structured and unstructured lattice options allow Round5 to address a variety of use cases.

Concerns were raised regarding the calculation of Round5 decryption and decapsulation failures. New parameters were suggested by the authors which appear to remedy this problem and the CCA-secure encryption scheme features failure rates reportedly below 2^{-128}. Round5 incorporates some internal building blocks that could use more documentation and security analysis and we hope that its selection as a second-round candidate will lead to more such analysis.

3.8 SABER

SABER is a family of lattice-based cryptographic primitives for PKE and unauthenticated KEMs, achieving CPA and CCA security based on the quantum hardness of the Module Learning with Rounding problem. The scheme uses modules of varying rank over a fixed power-of-2 cyclotomic ring with fixed dimension and modulus for security levels 1, 3, and 5. The MLWR secret distribution is the centered binomial distributio, and a hash of the session key is hashed with the public parameter for multi-target protection. Polynomial multiplication is specified using Toom-Cook and Karatsuba. CCA security is achieved by a variant of the Fujisaki-Okamoto transform. The session key is transported using an encryption-based approach for noisy key agreement.

SABER has very competitive performance among all candidates for post-quantum key exchange. In particular, it achieves one of the lower costs for bandwidth (public-key size plus ciphertext size) at each security level.

The most significant cryptanalytic concern for SABER is whether or not it is overstretching the

concrete hardness of (Module) Learning With Rounding. While there are no known (M)LWR-related attacks that exploit the chosen parameters, the reductions between bounded-sample MLWE and MLWR are rather loose and do not apply in SABER's case. We view SABER as an opportunity to highlight the need for (and benefit of) further analysis of (M)LWR with small parameters and bounded samples, in order to continue improving overall confidence in the assumption.

3.9 Three Bears

Three Bears is a variant of the module Learning with Errors problem. In this variant, instead of the underlying ring being a polynomial with an indeterminate x, the indeterminate x is evaluated, yielding instead a ring modulo an integer. As instantiated, this integer is a generalized Mersenne prime of special form. A major benefit of this choice is that it allows the use of already highly-optimized big integer arithmetic libraries and code, in particular libraries for the Ed448-Goldilocks elliptic curve.

Commented [MD(15]: Do we need to mention this?

NIST feels that Three Bears is just right for moving forward. The scheme appears to be one of the fastest submissions received by NIST, with very competitive key sizes. It also contains some much needed variety to the family of LWE-like schemes, and may be easier for non-experts to understand than some of the schemes that explicitly use algebraic number theory concepts.

Commented [MD(16]: Suggest removal

The specification would, however, benefit from some changes. It currently relies significantly on an unpublished e-print work for understandability. A more self-contained specification would be useful.

3.10 Classic McEliece

Classic McEliece is based on the well-known McEliece cryptosystem [15], the first code-based public-key cryptosystem published in 1978. The submission is for an IND-CCA2 KEM. The public key determines a random binary Goppa code, and generates a ciphertext by adding error to a codeword. Decapsulation is done by decoding. Security is based on the hardness of decoding a general linear code, and that a random binary Goppa code seems indistinguishable from a random linear code.

There is a long history of analysis of the security problem, which has not significantly altered the attack complexity. There are no known quantum attacks besides Grover's algorithm. As a result, there is a high degree of confidence in the security of Classic McEliece. Classic McEliece also has very short ciphertexts, on the order of 200 bytes, and seems to have good performance for encapsulation and decapsulation.

The main drawback to McEliece-type cryptosystems is the large public key size, which is over a million bytes. The submission only included parameter sets for category 5 security, so the submitters may wish to generate parameter sets for other security categories.

3.11 NTS-KEM

The NTS-KEM submission is quite similar to Classic McEliece, also being based on the original McEliece cryptosystem [15]. The candidate is an IND-CCA2 KEM, which has the same security

analysis as for Classic McEliece. Similarly, NTS-KEM has large public-keys, small ciphertexts, and seems to have good performance for encapsulation and decapsulation.

In contrast, there are a few differences between NTS-KEM and Classic McEliece. NTS-KEM generates their keys in a different way, and their specification has decryption failures. The NTS-KEM team provided parameters for security categories 1, 3, and 5, while Classic McEliece only has level 5. NTS-KEM could make their implementation constant time to provide more security against side-channel attacks.

3.12 BIKE

BIKE is a code-based KEM, combining three similar constructions that all use a bit-flipping decoder for a Quasi-Cyclic Moderate-Density-Parity-Check (QC-MDPC) code in their decapsulation algorithms. All three constructions are intended to be used ephemerally with a strict prohibition on key reuse – that is to say, they target IND-CPA security and make no attempt to make it difficult for an attacker to mount a chosen ciphertext attack if keys are reused. This design decision was made by the submitters, based on the difficulty of designing a bit-flipping decoder with a low enough decoding failure rate to allow an efficient IND-CCA2-secure construction.

BIKE offers key and ciphertext sizes and performance that are competitive with ring and module lattice schemes. From a security perspective, while the constructions used in BIKE are fairly new, dating from the 2010s, there are a number of features that increase confidence in their security: In particular, the schemes are structurally quite similar to well-studied lattice cryptosystems (BIKE I and II are similar to NTRU and BIKE III is similar to RLWE cryptosystems, substituting shortness in the Hamming metric for shortness in the Euclidean metric). BIKE also offers a security proof based on decisional variants of the Quasi-Cyclic Syndrome Decoding (QCSD) and Quasi-Cyclic Codeword Finding (QCCF) problems. Security strengths are based on information-set-decoding attacks, which may in fact be better understood than lattice attacks – information-set-decoding algorithms have only been incrementally improved since they were introduced over 50 years ago, and unlike lattice attacks there is good agreement between theory and experiment regarding their computational complexity.

Possible areas for further analysis related to BIKE include pursuing chosen ciphertext security by improving the decoding failure rate for QC-MDPC codes, investigating the relation between the search and decisional variants of the QCSD and QCCF problems, and investigating the effect, if any, of the quasi-cyclic code structure on security.

3.13 HQC

HQC is a code-based public key encryption scheme based on the hardness of a decisional version of the QCSD problem, targeting IND-CCA2 security. It uses a construction similar to RLWE, substituting shortness in the Hamming metric for shortness in the Euclidean metric, combined with a public error correction code.

Of the second-round candidate code-based cryptosystems, where information set decoding is the limiting attack for both private key recovery and message recovery (BIKE, HQC, and LEDAcrypt,) HQC has the strongest argument at present that its decryption failure rate is low

enough to obtain chosen-ciphertext security. However, it pays a significant penalty in key and ciphertext size in comparison to the others (although it still compares very favorably in key size and overall communication bandwidth to the candidate code-based cryptosystems based on Goppa codes.)

Early in the evaluation process, an attack on HQC was claimed based on the evaluation-at-one homomorphism of the underlying polynomial ring for HQC. However, the attack does not appear to succeed, as long as the second component of the ciphertext is truncated by at least one bit from the length of a full ring element. The second component of the ciphertext is in fact truncated, in the submitted version of HQC. Nonetheless, the claimed attack and the way it apparently fails highlight some important subtleties in the particular variant of decisional QCSD required for the security of HQC.

Commented [MD(17]: Shorten a tad?

Possible areas for further analysis related to HQC include investigating the relation between the search and decisional variants of the QCSD problem, and investigating the effect, if any, of the quasi-cyclic code structure on security.

3.14 LEDAcrypt (merger of LEDAkem and LEDApkc)

LEDAcrypt is a merger of two very similar code-based schemes, using quasi-cyclic Low-Density-Parity-Check (QC-LDPC) codes. The private parity check matrix for the public code is formed by multiplying the underlying QC-LDPC matrix by a similarly sparse square matrix. This results in a code which is quite similar to the QC-MDPC codes used in BIKE, but with some additional structure. While such codes could be decoded using a bit-flipping algorithm as in BIKE, LEDAcrypt instead uses a slightly different decoding algorithm called Q-decoding.

One area where LEDAcrypt may add value to the pool of second round candidates is in defending against chosen ciphertext attacks. While the submitted versions of LEDAkem and LEDApkc did not provide a low enough decryption failure rate to claim IND-CCA2 security according to the standards outlined in the NIST Call for Proposals [8], the parameters suggested for LEDAcrypt do claim a decryption failure rate that may be low enough. This is of interest, because, if these parameters can in fact be used to provide IND-CCA2 security, then they would significantly improve on the key and ciphertext sizes of HQC, the most similar scheme to LEDAcrypt that claims IND-CCA2 security.

Possible areas for further analysis related to LEDAcrypt include investigation of how the security of LEDAcrypt is affected by the additional structure of the underlying code in comparison to QC-MDPC codes, and whether the updated parameters really do give a low enough decryption failure rate to obtain IND-CCA2 security according to the standards of the NIST Call for Proposals [8].

3.15 Rollo (merger of LAKE, LOCKER, and Ouroboros-R)

Commented [MD(18]: Shorten slightly?

ROLLO is a merger combining the three rank-based first round submissions LAKE, LOCKER, and Ouroboros-R. The submitters have not suggested changing or eliminating any of the three constructions, but the merger will eliminate some redundancy between the three specifications. Each of the three merged schemes uses a decoding algorithm for ideal Low Rank Parity Check (LRPC) codes in its decryption or decapsulation algorithm. LAKE and LOCKER are based on an

NTRU-like construction, while Ouroboros-R is based on an RLWE-like construction, substituting the rank metric for the Euclidean metric in each case. The primary difference between LAKE and LOCKER is that LOCKER has adjusted its parameters to make the decryption failure rate low enough that it may claim IND-CCA2 security. The other two schemes only target IND-CPA security. Security proofs are provided based on decisional variants of the Ideal Rank Syndrome Decoding (IRSD) problem and the ideal LRPC distinguishing problem. LAKE and LOCKER require both assumptions, while Ouroboros-R only requires the former.

In cryptographic literature, rank-based cryptosystems like the component schemes of ROLLO are often grouped with code-based cryptosystems using the Hamming metric, but they are subject to significantly different cryptanalytic attacks. As such, including rank-based cryptosystems in our pool of second round candidates adds significant diversity. Moreover, the key size and overall bandwidth of LAKE are better than that of any other submitted lattice or code-based, for the same security against known attacks. Nonetheless, rank-based cryptography is quite new and not as well studied as lattice-based cryptography or code-based cryptography using the Hamming metric. More cryptanalysis on rank-based primitives would be valuable.

One particular area that could use more study is algebraic attacks targeting rank syndrome decoding and LRPC key recovery. Additionally, further study on separation or reduction between decisional and search variants of IRSD and LRPC key recovery/distinguishing may be of interest. Another area of cryptanalysis that needs more study, relevant to LOCKER in particular, is how decryption failures can be used to mount a chosen ciphertext attack and whether precomputation of ciphertexts by the adversary can be used to significantly increase the decryption failure rate. This will help determine how much performance and bandwidth penalty is required to attain chosen ciphertext security using the LAKE/LOCKER construction.

Finally, it should be mentioned that documentation for ROLLO as well as the documentation provided for the first-round submissions LAKE, LOCKER, and Ouroboros-R is somewhat sparse on details. For example, one should not have to look at the submitted code to know how an error support space is encoded as the input to a hash function. Lack of detail in specifications has not so far been a major consideration in NIST's evaluation of candidate algorithms, but it will become a larger concern as we get closer to the time when some submissions will need to be adapted into a fully specified NIST standard.

3.16 RQC

RQC is a rank-based public key encryption algorithm based on the hardness of a decisional version of the Ideal Rank Syndrome Decoding (IRSD) problem, targeting IND-CCA2 security. It uses a construction similar to ring-LWE, substituting shortness in the Rank metric for shortness in the Euclidean metric, combined with a public error correction code.

As RQC completely eliminates decryption failures and does not need to assume the hardness of the ideal LRPC distinguishing problem, it represents a more conservative approach to IND-CCA2 security than the LOCKER variant of ROLLO, which is the other rank-based second-round candidate algorithm targeting IND-CCA2 security, but comparatively suffers in decryption speed and ciphertext size.

One particular area of cryptanalysis that could use more study is algebraic attack targeting rank syndrome decoding. Additionally, further study on separation or reduction between decisional and search variants of IRSD may be of interest.

Like ROLLO, RQC could benefit from filling in some details in its specification, such as canonical encodings for support spaces and further specification of the use of public Gabidulin codes.

3.17 SIKE

SIKE was the only submission based on arithmetic properties of elliptic curves over finite fields. While quantum computers will break currently deployed elliptic curve cryptosystems, SIKE uses pseudo-random walks on supersingular isogeny graphs of curves, which are not known to be susceptible to quantum attacks. The nature of SIKE allows for a key exchange algorithm which is very similar to the classic Diffie-Hellman. The submission includes a CPA-secure encryption scheme which is converted to a CCA-secure KEM via a standard transformation.

SIKE has the smallest key sizes among all the remaining submissions, with public keys less than 750 bytes even for its level 5 security parameters. Another advantage of SIKE is that it can leverage existing optimized code for elliptic curve operations, and can thus be easily combined with traditional elliptic curve cryptography to create a hybrid classical/post-quantum scheme. The SIKE scheme also benefits from much research into protecting elliptic curve operations from side-channel attacks.

The basic security problem upon which SIKE relies, finding isogenies between supersingular elliptic curves, has not been studied as much of some of the security problems associated with other submissions. Another drawback is that the performance of SIKE seems to be an order of magnitude slower than many of the other candidates.

The digital signature schemes selected to move on include the following.

3.18 CRYSTALS-DILITHIUM

Dilithium is a lattice-based signature scheme, constructed using the Fiat-Shamir heuristic, whose security is based on the hardness of the MLWE problem. Dilithium is part of the CRYSTALS suite, together with the key exchange mechanism Kyber. The main novelty of Dilithium is that the size of the public key is reduced by omitting some of the low-order bits; to compensate for this, each signature includes an extra "hint" that allows the verifier to check the signature.

Dilithium offers fairly good performance, and is relatively straightforward to implement.

The best known attacks against Dilithium are based on lattice basis reduction, without making significant use of the algebraic structure of the MLWE problem. The parameter choices for Dilithium are based on conservative estimates of the costs of these attacks. Dilithium has a formal security proof in the classical random oracle model. This proof is nontrivial, and it breaks down in the quantum random oracle model, however no attacks are known.

Commented [MD(19]: Any suggestions for the Dilithium team?

3.19 FALCON

Falcon is a lattice-based signature scheme, based on GPV (Gentry-Peikert-Vaikuntanathan) Gaussian sampling, using the NTRU lattice. The main novelty is a very fast recursive algorithm for Gaussian sampling, using a tree data structure (the "Falcon tree").

Falcon offers very good performance. However, it is quite complicated to implement, as it relies heavily on the "tower of fields" structure of the number field. Also, Falcon requires double-precision floating-point arithmetic, which may not be available on small embedded processors. More work is needed to ensure that the signing algorithm is secure against side-channel attacks.

The best known attacks against Falcon are based on lattice basis reduction, without significantly exploiting the special structure of the NTRU lattice. Falcon has a formal security proof in the quantum random oracle model.

3.20 qTESLA

qTESLA is a lattice-based signature scheme which uses the assumption that RLWE distributions are indistinguishable from random. The public key in qTESLA is, roughly speaking, a sample of a RLWE distribution. The signer keeps secret information about this sample, and uses that information along with a hash function to produce signatures. Signature verification involves some simple arithmetic within the chosen ring, and then the recomputation of a hash function.

qTESLA has reasonably good performance parameters that are comparable to the other lattice-based signature schemes. The authors of qTESLA have claimed security proofs for the schemes in the random oracle model and the quantum random oracle model. These security proofs have some challenges: the original security proof had a bug that needed an adjustment in parameters, and the proof in the quantum random oracle model assumes (among other things) a conjecture about the distribution of random elements in the ring. NIST believes that the submission is substantial enough to warrant further analysis.

Commented [MD(20]: Any suggestions for qTesla?

3.21 GeMSS

GeMMS is a "big-field" multivariate digital signature scheme in the well-studied HFEv- (Hidden Field Equations) family. The scheme transforms the basic HFEv- design assumed to have existential unforgeability into a EUF-CMA secure signature scheme using the Feistel-Patarin construction. The existential unforgeability claim for the HFEv- design is loosely related to the well-studied MQ (multivariate quadratic) and MinRank problems.

GeMMS offers some of the smallest signature lengths among all submissions. GeMMS also benefits from the fact that the HFEv- construction is one of the most studied signature primitives in the literature.

Aside from signature size and verification time, other performance characteristics of GeMMS raise some concerns. The signing time is quite high and the public keys are quite large; these properties may be features of GeMMS that are inherent to the HFEv- methodology. Still, the security analyses suggest that there are possible tradeoffs among the degree bound, minus projection rank, and number of vinegar variables, for example, that may have an impact on

various performance characteristics. We hope as a second-round candidate that further optimizations can be found.

3.22 LUOV

LUOV is a "small-field" multivariate digital signature scheme based on the Unbalanced Oil and Vinegar (UOV) scheme. The main innovation of the scheme is to specify the public key as a map on a certain finite field while publishing coefficients on a subfield. The scheme avoids attacks directly exploiting the subfield structure by using a hash-and-sign approach, ensuring that the extension field must be used. The scheme also uses a pseudorandom generator to construct a part of the public key for which a corresponding private key portion can be solved, similar to the constructions in cyclic-UOV, cyclic-Rainbow and their pseudorandom counterparts.

LUOV offers an explicit tradeoff between key size and signature length, making the scheme flexible to disparate use cases. The scheme also has a message-recovery mode which conceivably may be of interest.

UOV has been a central object of study in multivariate cryptography for twenty years; thus, LUOV is derived from a seemingly solid foundation. The lifting innovation is very new, however, and could use more security analysis in the second round.

3.23 MQDSS

MQDSS is a multivariate digital signature scheme derived from a provably secure identification scheme based on the MQ problem. The signature scheme is constructed from the identification scheme via the application of a generalization of the Fiat-Shamir Transform appropriate for 5-pass identification schemes. We note explicitly that the proposed parameters do not satisfy the hypotheses of the security reduction.

MQDSS supports pseudorandom key generation with large signatures. The performance characteristics of MQDSS are most directly comparable to, and, depending on the security assumptions, are competitive with, those of hash-based signature schemes.

MQDSS could use more security analysis for the more aggressively chosen parameter sets. We expect that as a better understanding of boundary case security is developed that further optimization is possible. We hope that MQDSS will benefit from further research as a second-round candidate.

3.24 Rainbow

Rainbow is a multivariate digital signature scheme that is a generalization of the UOV structure allowing parameterizations that are more efficient at the cost of additional algebraic structure. The Rainbow signature in its format in this process has been studied for about fifteen years with various parameters. Rainbow claims EUF-CMA security utilizing a hash construction with a random salt.

The spectrum of Rainbow parameters allow for optimization in a diverse array of use cases. A further benefit of Rainbow is that it has also been studied in other contexts, including in

lightweight applications.

The Rainbow submission offers parameter sets targeting all of the security levels indicated in the NIST Call for Proposals [8]. As a second-round candidate, we expect that greater focus on a more narrow set of specifications will be reached. Furthermore, we hope that more research will be inspired on the collection of optimization techniques for Rainbow keys that exists in the literature and that was not considered in the Rainbow submission, ideally leading the community toward a consensus on their feasibility.

3.25 Picnic

Picnic is a signature scheme that uses no number-theoretic or structured hardness assumptions. The security reductions are to hash and symmetric block cipher. A Picnic signature is a non-interactive zero-knowledge proof of knowledge of the secret key. The plaintext being signed is incorporated (via hashing) into the challenges of the proof of knowledge in such a way that only the holder of the secret key can output the proof. The length of the signature depends on the multiplicative complexity of the encryption scheme and on the specific technique to construct a zero-knowledge proof of knowledge (from the field of secure multi-party computation).

Picnic is a highly modular design. The cryptographic primitives – hash and block cipher -- could be instantiated in different ways. The submitted design uses lowMC, a block cipher with low multiplicative complexity. LowMC has not been studied as much as AES. The effect of using AES instead of lowMC in Picnic seems to be an expansion of the signature length by a factor that ranges from 6 to 9, depending on the block size. Improvements in secure multi-party computation techniques would translate into smaller signatures. It is worth noting that the security requirements for the underlying block cipher are less stringent than the general security requirements of a block-cipher. This is because, in Picnic, a single (random plaintext, ciphertext) pair is ever revealed.

Commented [MD(21]: Add something about performance or suggestions for submitters?

3.26 SPHINCS+

SPHINCS$^+$ is a stateless hash-based signature scheme. Hash-based signature schemes were first proposed in late 1970s, and many improvements have been developed since then. SPHINCS$^+$ uses two different hash-based signature schemes: Winternitz One-Time Signature Plus (WOTS$^+$), a one-time signature scheme, and Forest of Random Subsets (FORS), a few-time signature scheme. A SPHINCS$^+$ key pair consists of 2^{60} or more FORS key pairs. Multiple levels of Merkle hash trees are used in order enable the individual FORS public keys to be authenticated. Each of the FORS public keys and the root of each of the Merkle hash trees is signed using WOTS$^+$. Messages are signed using a pseudorandomly selected FORS key, and a message signature consists of the FORS signature, one WOTS$^+$ signature for each Merkle tree level, and the intermediate hash values needed to traverse each Merkle tree.

Commented [MD(22]: Make slightly less technical?

The primary advantage of SPHINCS$^+$ is that its security relies solely on the preimage resistance of the hash function used. SPHINCS$^+$ also has very small public keys – 32 to 64 bytes, depending on the security level. The disadvantage is that signing is very slow and signatures are

relatively large, although SPHINCS$^+$ offers different parameter choices that trade off signature size for speed.

SPHINCS+ uses a pseudorandom function (PRF) to generate keys and bitmasks for each hash function call in order to protect against multi-target attacks against the hash function. Most of the cost of signature generation and verification is the time spent generating these keys and bitmasks. A possible second-round tweak might involve switching to a more efficient technique for protecting against multi-target attacks.

4 Conclusion and Next Steps

The announcement of the 26 second-round candidates BIKE, Classic McEliece, CRYSTALS-DILITHIUM, CRYSTALS-KYBER, FALCON, FrodoKEM, GeMSS, HQC, LAC, LEDAcrypt, LUOV, MQDSS, NewHope, NTRU, NTRU Prime, NTS-KEM, Picnic, qTESLA, Rainbow, ROLLO, Round5, RQC, SABER, SIKE, SPHINCS+, and Three Bears, marks the start of the second round of the NIST PQC Standardization Process. This report summarized the evaluation criteria used to select these candidate algorithms, and briefly described the basic design of the second-round candidates, along with advantages and disadvantages already noted in these submissions.

Submitters of the second-round candidates will be allowed to tweak their submissions to improve upon them if they wish, and fix any inconsistencies, problems or shortcomings in the specifications or source code. Any changes must be submitted to NIST by March 15, 2019 in a complete submission package, as defined in FRN-Dec16. More details will be provided on the webpage www.nist.gov/pqcrypto.

The next twelve to eighteen months will consist of a public review on the remaining 26 second-round post-quantum candidates. Some of the second-round candidates have received little or no published cryptanalysis by the cryptographic community-at-large. With the number of candidates substantially reduced from the first round, we hope that the combined efforts of the cryptographic community will evaluate the remaining candidates and provide NIST with feedback that supports or refutes the security claims of the submitters. We are also interested in additional performance data on each of the candidates. This includes optimized implementations written in assembly code or using instruction set extensions, and analyses of implementation suitability of candidate algorithms in constrained platforms, as well as performance data for hardware implementations.

NIST plans to host the Second NIST PQC Standardization Conference at the University of California Santa Barbara on August 22-24, 2019, following Crypto 2019. Submitters of the second-round candidates will be invited to present their algorithms. Sometime after the conference, NIST plans to either select finalists for a final round, or select a small number of candidates for standardization. More detailed plans will be provided at a later date.

Appendix A—References

[1] U.S. Department of Commerce. *Digital Signature Standard (DSS)*, Federal Information Processing Standards (FIPS) Publication 186-4, July 2013, 121pp. https://doi.org/10.6028/NIST.FIPS.186-4.

[2] NIST Special Publication (SP) 800-56A Revision 3, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography,* National Institute of Standards and Technology, Gaithersburg, Maryland, April 2018, 141pp. https://doi.org/10.6028/NIST.SP.800-56Ar3.

[3] NIST Special Publication (SP) 800-56B Revision 1, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography,* National Institute of Standards and Technology, Gaithersburg, Maryland, September 2014, 121pp. https://doi.org/10.6028/NIST.SP.800-56Br1.

[4] NIST Workshop on Cybersecurity in a Post-Quantum World, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2-3, 2015, https://csrc.nist.gov/Events/2015/Workshop-on-Cybersecurity-in-a-Post-Quantum-World.

[5] L. Chen, S. Jordan, Y.K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-tone, *Report on Post-Quantum Cryptography*, NISTIR 8105, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016, 10pp. https://doi.org/10.6028/NIST.IR.8105.

[6] D. Moody, *Post-Quantum Cryptography Standardization: Announcement and outline of NIST's Call for Submissions*, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, https://csrc.nist.gov/Presentations/2016/Announcement-and-outline-of-NIST-s-Call-for-Submis.

[7] "Post-Quantum Cryptography: Proposed Requirements and Evaluation Criteria," 81 *Federal Register* 50686 (August 2, 2016), pp. 50686-50687. https://federalregister.gov/a/2016-18150.

[8] "Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms," 81 *Federal Register* 92787 (December 20, 2016), pp. 92787-92788. https://federalregister.gov/a/2016-30615.

[9] "Establishment of NIST Smart Grid Advisory Committee and Solicitation of Nominations for Members," 75 *Federal Register* 7 (January 12, 2010), pp. 1595-1596. https://federalregister.gov/a/2010-344 [accessed 2/25/14].

[10] U.S. Department of Commerce. *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information Processing

Standards (FIPS) Publication 197, November 2001, 47pp. https://doi.org/10.6028/NIST.FIPS.197.

[11] U.S. Department of Commerce. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions)*, Federal Information Processing Standards (FIPS) Publication 202, August 2015, 29pp. https://doi.org/10.6028/NIST.FIPS.202.

[12] NIST pqc-forum mailing list 2018-05-04, Jacob Alperin-Sheriff, https://groups.google.com/a/list.nist.gov/d/msg/pqc-forum/xFxHuxPXTO4/wZCFL734AQAJ.

[13] D. Moody, *Let's Get Ready to Rumble – The NIST PQC "Competition"*, PQCrypto 2018, Ft. Lauderdale, Florida, April 11, 2018, https://csrc.nist.gov/Presentations/2018/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti.

[14] J. Hoffstein, J. Pipher, and J.H. Silverman, *NTRU: A ring-based public key cryptosystem*, in ANTS, Lecture Notes in Comput. Sci. 423, J. Buhler, ed., Springer, Berlin, 1998, pp. 267-288.

[15] R. McEliece, *A public-key cryptosystem based on algebraic coding theory*, DSN Progress Report 42-44, Jet Propulsion Laboratory, Pasadena, CA, 1978. http://ipnpr.jpl.nasa.gov/progressreport2/42-44/ 44N.pdf.