From: Peralta, Rene (Fed)
To: (b) (6)
Subject: Fw: PQC docs
Date: Wednesday, October 26, 2016 4:03:56 PM
Attachments: final CFP v4-YKL.docx
FAQ 2-YKL.docx

From: Liu, Yi-Kai (Fed)
Sent: Wednesday, October 26, 2016 3:22 PM
To: Perlner, Ray (Fed); Chen, Lily (Fed); Moody, Dustin (Fed); Daniel Smith-Tone; Alperin-Sheriff, Jacob (Fed)
Cc: Peralta, Rene (Fed); Jordan, Stephen P (Fed); Bassham, Lawrence E (Fed)
Subject: Re: PQC docs

Hi everyone,

I made some edits to the CFP and FAQ, mainly having to do with quantum security.

Ray, I didn't change any of your meanings, I just revised the text to make it clearer. What do you think?

In particular, I'm much more comfortable now with your approach to measuring quantum security. But it really requires a lot of explanation to see why it makes sense. This was hard to follow in the earlier drafts of the CFP and the FAQ, but I think it is much clearer now.

Lily, sorry I didn't see your comments while I was editing the draft. Anyway, we can still edit some more.

--Yi-Kai

From: Perlner, Ray (Fed)
Sent: Wednesday, October 26, 2016 2:05 PM
To: Chen, Lily (Fed); Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Daniel Smith-Tone; Alperin-Sheriff, Jacob (Fed)
Cc: Peralta, Rene (Fed); Jordan, Stephen P (Fed); Bassham, Lawrence E (Fed)
Subject: RE: PQC docs

1) KEM-KWS is actually using the KEM terminology the same way as we are using it in the CFP. Specifically it is a KEM combined with a key wrapping scheme to make a public key encryption scheme. The KEM is composed of RSASVE and an approved KDF. Again, while RSA-KEM-KWS is not itself a KEM, it is composed of two components, one of which is a KEM, and the other of which is a KWS.

2) Security strength 2 does not mean 0% Groverizer effect. If there is a larger Groverizer effect, it simply means that you need more classical security than 128 bits to get the appropriate quantum security.

From: Chen, Lily (Fed)
Sent: Wednesday, October 26, 2016 11:58 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Daniel Smith-Tone <daniel-c.smith@louisville.edu>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-

sheriff@nist.gov>
Cc: Peralta, Rene (Fed) <rene.peralta@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Subject: Re: PQC docs

Attached please see my comments on CFPv4. I noticed that we added a fairly amount of details and explanations. The details and explanations help people understand what we are asking for. On the other hand, the details often need to be handled more carefully and think about the impacts. Here are two places I feel we shall check.

1. KEM concept. In the current draft, we consider an ephemeral DH like scheme (e.g. New Hope) as a KEM. Then converting KEM to a public-key encryption is not intuitive at all. I cannot see why we need it other than security proofs. The recipient will need to send something in order to receive "public key encrypted" something. Usually, for public key encryption, we use static public key, not ephemeral public key. Furthermore, we have to assume an authenticated encryption (like GCM), which in my opinion, is not very reasonable. What we really need is (1) public key encryption (use either ephemeral or static public key) (2) Key agreement (like ephemeral DH). In practice, we may need to convert (1) to (2) (use one time public key), not from (2) to (1).

Please notice that, in 56B KEM-KWS is to use RSA to "encapsulate" a value, then derive a key from the "value" and used it to do key wrap. The KEM in 56B is different from what we called KEM.

2. Quantum security levels (1, 3, 5) vs. (2, 4).

I understand that for two algorithms A and B with parameter sets providing 128 bit classical security. If A satisfies level 1 quantum security while B satisfies level 2 quantum security, then we are in favor of algorithm B. However, A and B must be from different families, they will not be compared only on quantum security levels in the future but other properties. I also feel that level 2 is a special case of level 1. Level 1 means Groverizer effect less than 100%, assuming 100% is to make square root of classical security level, while Level 2 means Groverizer effect equal to 0% meaning no effect at all. Again, a give algorithm will fit into either (1, 3, 5) or (2, 4) with parameter choices. A given algorithm will never reasonably provide 1, 2, 3, 4, 5 levels with different selection of parameters. Introducing levels 2 and 4 complicated our statement.

Let's think about.

Lily

_____

From: Moody, Dustin (Fed)
Sent: Tuesday, October 25, 2016 12:56:27 PM
To: Perlner, Ray (Fed); Liu, Yi-Kai (Fed); Daniel Smith-Tone; Alperin-Sheriff, Jacob (Fed)
Cc: Peralta, Rene (Fed); Jordan, Stephen P (Fed); Chen, Lily (Fed); Bassham, Lawrence E (Fed)
Subject: PQC docs

Ray, Daniel, Jacob, and Yi-Kai,
Attached are the most recent versions of the FAQ and CFP. Please use them as you edit. Here are the assignments:
Daniel – edit your FAQ bullet
Ray – write a post summarizing our approach to quantum security in the CFP for the pqc-forum
Yi-Kai – edit Ray's FAQ bullets on quantum security, in addition to 4.A.5
Dustin – write a post summarizing our changes dealing with KEMs, along with the API to be posted in the pqc-forum
Jacob – write a summary of the comments and how we responded to them

Daniel, Ray, Yi-Kai (and myself). Please get these done this week. Next week we hit November. Thanks!

Dustin

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

Table of Contents

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

our current public-key cryptosystems to prepare for the event that large-scale quantum computers become a reality.

At present, there are several post-quantum cryptosystems that have been proposed, including lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems, hash-based signatures, and others. However, for most of these proposals, further research is needed in order to gain more confidence in their security (particularly against adversaries with quantum computers) and to improve their performance.

NIST has decided that it is prudent to begin developing standards for post-quantum cryptography now. This is driven by two factors. First, there has been noticeable progress in the development of quantum computers, including theoretical techniques for quantum error correction and fault-tolerant quantum computation, and experimental demonstrations of physical qubits and entangling operations in architectures that have the potential to scale up to larger systems.

Second, it appears that a transition to post-quantum cryptography will not be simple as there is unlikely to be a simple "drop-in" replacement for our current public-key cryptographic algorithms. A significant effort will be required in order to develop, standardize, and deploy new post-quantum cryptosystems. In addition, this transition needs to take place well before any large-scale quantum computers are built, so that any information that is later compromised by quantum cryptanalysis is no longer sensitive when that compromise occurs. Therefore, it is desirable to plan for this transition early.

NIST is beginning a process to develop new post-quantum cryptography standards, including digital signature schemes specified in Federal Information Processing Standards Publication (FIPS) 186 and key establishment schemes specified in NIST Special Publications (SP) 800-56 A and B. The process is referred to as *post-quantum cryptography standardization*. The standards will be published as Federal Information Processing Standards (FIPSs) or Special Publications (SPs).

NIST is soliciting proposals for post-quantum cryptosystems and it will solicit comments from the public as part of its evaluation process. NIST expects to perform multiple rounds of evaluation, over a period of three to five years. The goal of this process is to select a number of acceptable candidate cryptosystems for standardization.

NIST anticipates that the evaluation process for these post-quantum cryptosystems may be significantly more complex than the evaluation of the SHA-3 and AES candidates. One reason is that the requirements for public-key encryption and digital signatures are more complicated. Another reason is that the current scientific understanding of the power of quantum computers is far from comprehensive. Finally, some of the candidate post-quantum cryptosystems may have completely different design attributes and mathematical foundations, so that a direct comparison of candidates would be difficult or impossible.

As a result of these complexities, NIST believes that its post-quantum standards development process should not be treated as a competition; in some cases, it may not be possible to make a well-supported judgment that one candidate is "better" than another. Rather, NIST will perform a thorough analysis of the submitted algorithms in a manner that is open and transparent to the public, as well as encourage the cryptographic community to also conduct analyses and evaluation. This combined analysis will inform NIST's decision on the subsequent development of post-quantum standards.

NIST recognizes that some users may wish to deploy systems that use "hybrid modes," which combine post-quantum cryptographic algorithms with existing cryptographic algorithms (which may not be post-quantum). These "hybrid modes" are outside of the scope of this document, which is focused on post-quantum cryptographic algorithms only.

2. Proposed Requirements for the Submission Packages

Submission packages must be received by NIST by November 30, 2017. Submission packages received before September 30, 2017 will be reviewed for completeness by NIST; the submitters will be notified of any deficiencies by October 31, 2017, allowing time for deficient packages to be amended by the submission deadline. No amendments to packages will be permitted after the submission deadline, except at specified times during the evaluation phase (see Section 5).

Due to the specific requirements of the intellectual property statements as specified in Section 2.D, e-mail submissions will not be accepted for these statements The statements specified in Section 2.D must be mailed to Dustin Moody, Information Technology Laboratory, Attention: Post-Quantum Cryptographic Algorithm Submissions, 100 Bureau Drive – Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, or can be given to NIST at the first PQC Standardization Conference (see Section 5.C). The remainder of the submission package can either be mailed with the intellectual property statements, or sent as email to: pqc-submissions@nist.gov.

"Complete and proper" submission packages will be posted at http://www.nist.gov/pqcrypto for review. To be considered as a "complete" submission, packages must contain the following:

- Cover Sheet.
- Algorithm Specifications and Supporting Documentation.
- Optical Media.
- Intellectual Property Statements / Agreements / Disclosures.

These requirements are detailed below.

To be considered as a "proper" submission, packages must meet the minimum acceptability requirements specified in Section 3.

2.A Cover Sheet

The cover sheet of a submission package shall contain the following information:

- Name of the proposed cryptosystem.
- Principal submitter's name, e-mail address, telephone, organization, and postal address.
- Name(s) of auxiliary submitter(s).
- Name of the inventor(s)/ developer(s) of the cryptosystem.
- Name of the owner, if any, of the cryptosystem (normally expected to be the same as the submitter).
- Signature of the submitter.
- (optional) Backup point of contact (with telephone, fax, postal address, and e-mail address).

2.B Algorithm Specifications and Supporting Documentation

Each submission must include:

1) a complete written specification
2) a detailed performance analysis
3) Known Answer Test values
4) a thorough description of the expected security strength
5) an analysis of the algorithm with respect to known attacks
6) a statement of advantages and limitations.

Further details are described below.

2.B.1

A complete written specification of the algorithms shall be included, consisting of all necessary mathematical operations, equations, tables, and diagrams that are needed to implement the algorithms. The document shall also include a design rationale, and an explanation for all the important design decisions that have been made.

Each submission package shall describe a collection of algorithms, also called a cryptosystem or cryptographic scheme, that implements one or more of the following functionalities: public-key encryption, key encapsulation mechanism[1] (KEM), and digital signature. Public-key encryption schemes shall include algorithms for key generation, encryption, and decryption. KEM schemes shall include algorithms for key generation, encapsulation, and decapsulation. Digital-signature schemes shall include algorithms for key generation, signature generation and signature verification.

If a submission includes more than one type of scheme, NIST will evaluate the schemes of each type separately. Submitters may choose to combine different types of schemes into a single submission. They may also instead prepare and submit a complete

[1] In SP 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, KEMs are noted to be schemes, and are not to be considered protocols.

submission package for each algorithm, making sure to include all supporting documents and intellectual property statements in each individual package.

As the KEM and public key encryption functionalities can generally be interconverted, unless the submitter specifies otherwise, NIST will apply standard conversion techniques to public key encryption algorithms, so that the resulting scheme can be considered for standardization as a KEM, and vice versa: To convert a public key encryption function to a KEM, NIST will construct the encapsulate function by generating a random key and encrypting it. (The key generation and decapsulation functions of the KEM will be the same as the key generation and decryption functions of the original public key encryption scheme.) To convert a KEM to a public key encryption scheme, NIST will construct the encryption function, by appending to the KEM ciphertext, an AES-GCM ciphertext of the plaintext message, with a randomly generated IV. The AES key will be the symmetric key output by the encapsulate function. (The key generation function will be identical to that for the original KEM, and the decryption function will be constructed by decapsulation followed by AES decryption.)

Commented [PR(1]: RP: See added text. I still think we should put this in code somewhere.

For algorithms that have tunable parameters (such as the dimension of some underlying vector space, or the number of equations and variables), the submission document shall specify concrete values for these parameters. If possible, the submission should specify several parameter sets that allow the selection of a range of possible security/performance tradeoffs. In addition, the submitter should provide an analysis of how the security and performance of the algorithms depend on these parameters. To facilitate the analysis of these algorithms by the cryptographic community, submitters are encouraged to also specify parameter sets that provide lower security levels, and to provide concrete examples that demonstrate how certain parameter settings affect the feasibility of known cryptanalytic attacks.

Specific parameter sets may permit NIST to select a different performance/security tradeoff than originally specified by the submitter, in light of discovered attacks or other analysis, and in light of the alternative algorithms that are available. NIST will consult with the submitter of the algorithm, as well as the cryptographic community, if it plans to select that algorithm for development as a NIST standard, but with a different parameter set than originally specified by the submitter.

A complete submission shall specify any padding mechanisms and any uses of NIST-approved cryptographic primitives that are needed in order to achieve security. If the scheme uses a cryptographic primitive that has not been approved by NIST, the submitter shall provide an explanation for why a NIST-approved primitive would not be suitable.

To help rule out the existence of possible back-doors in an algorithm, the submitter shall explain the provenance of any constants or tables used in the algorithm.

2.B.2 The submitter must also include a statement regarding the algorithm's estimated computational efficiency and memory requirements for the "NIST PQC Reference Platform" (specified in Section 5.B). Efficiency estimates for other platforms may be

included at the submitter's discretion. These estimates shall each include the following information, at a minimum:

a. A description of the platform used to generate the estimate, in sufficient detail so that the estimates could be verified in the public evaluation process. For software implementations, include information about the processor, clock speed, memory, and operating system, on which the performance estimates were obtained. For hardware estimates, a gate count (or estimated gate count) should be included.

b. A speed estimate and memory requirements for the algorithm(s) on the reference platform specified in Section 5.B. At a minimum, the number of milliseconds or clock cycles required to perform each required operation (e.g., key generation, encryption, decryption, sign, verify), and the size of all inputs and outputs (e.g., keys, ciphertexts, signatures).

2.B.3 In addition, each submission package is required to include Known Answer Test (KAT) values that can be used to determine the correctness of an implementation of the submitted algorithms. The KATs are individual input tuples that produce single output values, e.g., an input tuple of a key and plaintext resulting in an output of the corresponding ciphertext. If an algorithm uses random values, the KAT should specify a fixed value for the random bits used by the algorithm, in order to force the algorithm to produce a fixed output value. Separate KATs should be provided to test different aspects of the algorithm, e.g., key generation, encryption, decryption, sign, verify, etc.

The KATs shall be included as specified below. All of these KAT values shall be submitted electronically, in separate files, on a CD–ROM, DVD, USB flash drive, or included in a zip file as described in Section 2.C.

Each file must be clearly labeled with header information listing:

1. Algorithm name,
2. Test name,
3. Description of the test, and
4. Other parameters.

The list must be followed by a set of tuples where all values within the tuple are clearly labeled (*e.g.*, Plaintext, PublicKey, RandomBits, Ciphertext, etc.). Sample files for these KAT values will be posted at http://www.nist.gov/pqcrypto.

All applicable KATs that can be used to verify various features of the algorithm shall be included. A set of KATs shall be included for each security strength specified in Section 4.A. Required KATs include:

a) If the execution of an algorithm produces intermediate results that are informative (e.g., for debugging an implementation of the algorithm), then the submitter shall include known answers for those intermediate values for each of the required security

strengths. Examples of providing such intermediate values are available at: http://csrc.nist.gov/groups/ST/toolkit/index.html.

b) If tables are used in an algorithm, then a set of KAT vectors shall be included to make use of the table entries.

Note: The submitter is encouraged to include any other KATs that test different features of the algorithm (e.g., for permutation tables, padding scheme, etc.). The purposes of these tests shall be clearly described in the file containing the test values.

2.B.4 The submission package shall include a statement of the expected security strength of the cryptosystem, along with a supporting rationale. For each parameter set the submitter wishes NIST to consider for standardization, the submitter shall specify a security definition from sections 4.A.2, 4.A.3, or 4.A.4, as well as an estimated security strength according to the categories given in section 4.A.5. All submitters are advised to be somewhat conservative in assigning parameters to a given category, but submitters of algorithms where the complexity of the best known attack has recently decreased significantly, or is otherwise poorly understood, should be especially conservative. Submitters should give quantitative estimates for any additional security provided by their settings above and beyond the minimum security strength provided by the relevant security strength category. Such estimates should include, at a minimum, a claimed classical security strength. Furthermore, the statement should address the additional attack scenarios identified in Section 4.A.6.

Commented [PR(2]: This was a "should", I think this should be a "shall"

2.B.5 The submission package shall include a statement that summarizes the known cryptanalytic attacks on the scheme, and provides estimates of the complexity of these attacks.

The submitter shall provide a list of references to any published materials describing or analyzing the security of the submitted algorithm or cryptosystem. When possible, the submission of copies of these materials (accompanied by a waiver of copyright or permission from the copyright holder for public evaluation purposes) is encouraged.

2.B.6 The submission package shall include a statement that lists and describes the advantages and limitations of the cryptosystem. Such advantages and limitations may involve the assessment of the cryptosystem's security against classical and quantum attacks, as well as any unusual characteristics of the scheme, such as extra functionalities, performance tradeoffs, and unusual vulnerabilities. This statement may also discuss the ease of implementing and deploying the algorithms, and their compatibility with existing protocols, networks and applications. This could include, for example, the suitability of the algorithm for use in hybrid schemes, which may be part of the transition to post-quantum cryptosystems.

In addition, this statement may address the ability to implement the algorithms in various environments, including, but not limited to 8-bit processors (e.g., smartcards), voice applications, satellite applications, or other environments where low power, constrained

memory, or limited real-estate are consideration factors. To demonstrate the efficiency of a hardware implementation of the algorithm, the submitter may include a specification of the algorithm in a nonproprietary hardware description language (HDL).

2.C Digital and Optical Media

All electronic data shall be provided either in a zip file, or on a single CD-ROM, DVD, or USB flash drive labeled with the submitter's name, as well as the name of the proposed cryptosystem.

2.C.1 Implementations Two implementations are required in the submission package: a reference implementation and an optimized implementation. The goal of the reference implementation is to promote understanding of how the submitted algorithm may be implemented. Since this implementation is intended for reference purposes, clarity in the implementation code is more important than the efficiency of the code. The reference implementation should include appropriate comments and clearly map to the algorithm description included in Section 2.B.1. The optimized implementation, targeting the Intel x64 processor (a 64-bit implementation), is intended to demonstrate the performance of the algorithm. Both implementations shall consist of source code written in ANSI C.

Both implementations shall be capable of fully demonstrating the operation of the proposed algorithm. This includes support for all core features of the algorithm, e.g., encryption, decryption, key generation, public-key validation, shared secret generation, and digital signature generation and verification.

A separate document specifying a set of cryptographic service calls, i.e. a cryptographic API, for the ANSI C implementations, will be made available at http://www.nist.gov/pqcrypto. Both the reference implementation and the optimized implementation shall adhere to the provided API. Separate source code for implementing the KATs shall also be included and shall adhere to the provided API.

The reference implementation shall be provided in a directory labeled: Reference_Implementation.

The optimized implementation shall be provided in a directory labeled: Optimized_Implementation.

Submitters may, at their discretion, submit additional implementations for other platforms. These implementations may be useful during the evaluation process.

2.C.2 Known Answer Tests The files included in the zip file or on the CD–ROM, DVD, or USB flash drive shall contain all of the required test values as specified in Section 2.B.3.

These test values shall be provided in a directory labeled: KAT.

2.C.3 Supporting Documentation To facilitate the electronic distribution of submissions to all interested parties, copies of all written materials must also be submitted in electronic form in the PDF file format. Submitters are encouraged to use the thumbnail and bookmark features, to have a clickable table of contents (if applicable), and to include other links within the PDF as appropriate.

The electronic version of the supporting documentation shall be provided in a directory labeled: Supporting_Documentation.

2.C.4 General Requirements for Digital and Optical Media For the portions of the submission that may be provided electronically, the information shall be provided using the ISO 9660 format. This media shall have the following structure:

- README
- Reference_Implementation
- Optimized_Implementation
- KAT
- Supporting_Documentation

The "README" file shall be a plain text file and list all files that are included on the disc with a brief description of each.

All optical media presented to NIST must be free of viruses or other malicious code. The submitted media will be scanned for the presence of such code. If malicious code is found, NIST will notify the submitter and ask that a clean version of the optical media be submitted.

2.D Intellectual Property Statements / Agreements / Disclosures

Each submitted algorithm, together with each submitted reference implementation and optimized implementation, must be made freely available for public review and evaluation purposes worldwide during the period of the post-quantum algorithm search and evaluation. The following signed statements will be required for a submission to be considered complete: 1) statement by the submitter, 2) statement by patent (and patent application) owner(s) (if applicable), and 3) statement by reference/optimized implementations' owner(s). Note that for the last two statements, separate statements must be completed if multiple individuals are involved.

Given the nature and use of cryptographic algorithms, NIST's PQC goals include identifying technically robust algorithms and facilitating their widespread adoption. NIST does not object in principle to algorithms or implementations which may require the use of a patent claim, where technical reasons justify this approach.

NIST has observed that royalty-free availability of cryptosystems and implementations has facilitated adoption of cryptographic standards in the past. As part of its evaluation of a PQC cryptosystem for standardization, NIST will consider the assurances made in the statements by the submitter(s) and any patent owner(s), with a strong preference for

submissions as to which there are commitments to license, without compensation, under reasonable terms and conditions that are demonstrably free of unfair discrimination.

2.D.1 Statement by Each Submitter

I, _____ (print submitter's full name) _____, of _____(print full postal address)_____ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

- ☐ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____;* ***OR*** *(check one or both of the following):*
  - ☐ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
  - ☐ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) _____.*

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:
Title:
Date:
Place:

2.D.2 Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner, or each owner's authorized representative, of each patent and patent application identified.

I, _____ (print full name) _____ , of _____(print full postal address)_____ , am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): _____ (enumerate) _____ , and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as _____(print name of cryptosystem) _____ is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):

- ☐ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

- ☐ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer

documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:
Title:
Date:
Place:

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, _____ (print full name) _____ , (print full postal address)_____ , am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed:
Title:
Date:
Place:

2.E General Submission Requirements

NIST welcomes both domestic and international submissions; however, in order to facilitate analysis and evaluation, it is required that the submission packages be in English. This requirement includes the cover sheet, algorithm specification and supporting documentation, source code, and intellectual property information. Any required information that is not submitted in English shall render the submission package "incomplete." Optional supporting materials (e.g., journal articles) in another language may be submitted.

Classified and/or proprietary submissions will not be accepted.

2.F Technical Contacts and Additional Information

For technical inquiries, send e-mail to pqc-comments@nist.gov, or contact Dustin Moody, National Institute of Standards and Technology, 100 Bureau Drive—Stop 8930, Gaithersburg, MD 20899–8930; telephone: +1 301–975–8136 or via fax at +1 301–975–8670, e-mail: dustin.moody@nist.gov.

Answers to germane questions will be posted at http://www.nist.gov/pqcrypto. Questions and answers that are not pertinent to this announcement may not be posted. NIST will endeavor to answer all questions in a timely manner.

3. Proposed Minimum Acceptability Requirements

Those submission packages that are deemed by NIST to be "complete" will be evaluated for the inclusion of a "proper" post-quantum public-key cryptosystem. To be considered as a "proper" post-quantum public-key cryptosystem (and continue further in the standardization process), the scheme shall meet the following 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 Sections 2.D.1, 2.D.2 and 2.D.3, as applicable.
2. The algorithms shall not incorporate major components that are believed to be insecure against quantum computers. (For example, hybrid schemes that include encryption or signatures based on factoring or discrete logs will not be considered for standardization by NIST in this context.)
3. The algorithms shall provide at least one of the following functionalities: public-key encryption, key exchange, or digital signature:
   a. Public-key encryption schemes 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.
   b. KEM schemes 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.
   c. Digital-signature schemes shall include algorithms for key generation, signature, and 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.

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.)

A submission package that is complete (as defined in Section 2) and meets the minimum acceptability requirements (as defined immediately above) will be deemed to be a "complete and proper" submission. A submission that NIST deems otherwise at the close of the submission period will receive no further consideration. Submissions that are "complete and proper" will be posted at http://www.nist.gov/pqcrypto for public review.

4. Proposed Evaluation Criteria

NIST will form an internal selection panel composed of NIST employees to analyze the submitted algorithms; the evaluation process will be discussed in Section 5. All of NIST's analysis results will be made publicly available.

Although NIST will be performing its own analyses of the submitted algorithms, NIST strongly encourages public evaluation and publication of the results. NIST will take into account its own analysis, as well as the public comments that are received in response to the posting of the "complete and proper" submissions, to make its decisions.

To avoid unnecessary duplication of effort, and to streamline the evaluation process, NIST encourages researchers who are developing similar cryptosystems to combine their efforts and produce a single submission package.

4.A Security

The security provided by a cryptographic scheme is the most important factor in the evaluation. Schemes will be judged on the following factors:

4.A.1 Applications of Public-Key Cryptography NIST intends to standardize post-quantum alternatives to its existing standards for digital signatures (FIPS 186) and key establishment (SP 800-56A, SP 800-56B). These standards are used in a wide variety of Internet protocols, such as TLS, SSH, IKE, IPsec, and DNSSEC. Schemes will be evaluated by the security they provide in these applications, and in additional applications that may be brought up by NIST or the public during the evaluation process. Claimed applications will be evaluated for their practical importance if this evaluation is necessary for deciding which algorithms to standardize.

4.A.2 Security Definition for Encryption/Key-Establishment
One particularly important application of public-key cryptography is to securely establish a key to be used for symmetric encryption. In previous publications [SP800-57], NIST has distinguished between two methods of achieving this functionality. The first method uses public-key encryption algorithms (such as RSA), known in this context as key

transport algorithms, while the second uses KEMs (such as Diffie-Hellman), known in this context as key agreement or key exchange. NIST expects submitters of encryption and KEM schemes to be aware of this application. NIST intends to standardize one or more schemes that enable "semantically secure" encryption or key encapsulation with respect to adaptive chosen ciphertext attack, for general use. This property is generally denoted *IND-CCA2 security* in academic literature.

The above security definition should be taken as a statement of what NIST will consider to be a relevant attack. Submitted KEM and encryption schemes will be evaluated based on how well they appear to provide this property, when used as specified by the submitter. Submitters are not required to provide a proof of security, although such proofs will be considered if they are available.

For the purpose of estimating security strengths, it may be assumed that the attacker has access to the decryptions of no more than 2^{64} chosen ciphertexts; however, attacks involving more ciphertexts may also be considered. Additionally, it should be noted that NIST is primarily concerned with attacks that use classical (rather than quantum) queries to the decryption oracle or other private-key functionality.

4.A.3 Security Definition for Ephemeral-Only Encryption/Key-Establishment While chosen ciphertext security is necessary for many existing applications (for example, nominally ephemeral key exchange protocols that allow key caching), it is possible to implement a purely ephemeral key exchange protocol in such a way that only passive security is required from the encryption or KEM primitive.

For these applications, NIST will consider standardizing an encryption or KEM scheme which provides semantic security with respect to chosen plaintext attack. This property is generally denoted *IND-CPA security* in academic literature.

The above security definition should be taken as a statement of what NIST will consider to be a relevant attack. Submitted KEM and encryption schemes will be evaluated based on how well they appear to provide this property, when used as specified by the submitter. Submitters are not required to provide a proof of security, although such proofs will be considered if they are available. Any security vulnerabilities that result from re-using a key should be fully explained.

4.A.4 Security Definition for Digital Signatures NIST intends to standardize one or more schemes that enable existentially unforgeable digital signatures with respect to an adaptive chosen message attack. (This property is generally denoted *EUF-CMA security* in academic literature.)

The above security definition should be taken as a statement of what NIST will consider to be a relevant attack. Submitted algorithms for digital signatures will be evaluated based on how well they appear to provide this property when used as specified by the submitter. Submitters are not required to provide a proof of security, although such proofs will be considered if they are available.

For the purpose of estimating security strengths, it may be assumed that the attacker has access to signatures for no more than 2^{64} chosen messages; however, attacks involving more messages may also be considered. Additionally, it should be noted that NIST is primarily concerned with attacks that use classical (rather than quantum) queries to the signing oracle.

4.A.5 Security Strength Categories NIST anticipates that there will be significant uncertainties in estimating the security strengths of these post-quantum cryptosystems. These uncertainties come from two sources: first, the possibility that new quantum algorithms will be discovered, leading to new cryptanalytic attacks; and second, our limited ability to predict the performance characteristics of future quantum computers, such as their cost, speed and memory size.

In order to address these uncertainties, NIST proposes the following approach. Instead of asking for precise estimates of the number of "bits of security," NIST proposes a set of minimum requirements for security strength. NIST recommends that submitters exceed these minimum requirements by some suitable margin, in order to account for possible uncertainties in their own estimates of security strength. Furthermore, NIST is formulating these minimum requirements in a way that will ensure security in a variety of scenarios, representing a broad range of possibilities regarding the future development of both classical and quantum computing technologies. NIST understands that this will require submitters to perform a more thorough analysis than has been done in most previous research.

For purposes of standardization, NIST proposes a collection of different security strength categories. A given cryptosystem may be instantiated using different parameter sets in order to fit into different categories. ~~NIST will classify submitted parameter sets based on the computational cost of attacking them under a variety of plausible scenarios regarding future progress in classical and quantum computing.~~ The goals of this classification are:

1) To facilitate meaningful performance comparisons between the submitted algorithms, by ensuring, insofar as possible, that the parameter sets being compared provide comparable security.
2) To allow NIST to make consistent and sensible future decisions regarding when to transition to longer keys.
3) To better understand the security/performance tradeoffs involved in a given design approach.

In accordance with the second goal above, NIST will base its classification on the range of security strengths offered by the existing NIST standards in symmetric cryptography, which NIST expects to offer significant resistance to quantum cryptanalysis. In particular, NIST will define a separate category for each of the following security requirements (listed in order of increasing strength): ~~NIST will classify the parameter sets being considered for standardization into the following categories:~~

Commented [LY(3]: I added this introduction, to give some general motivation before getting into the detailed definition of the 5 security categories

1) ~~Violating the relevant security definition requires~~Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g. AES128)
2) ~~Violating the relevant security definition requires~~ Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256)
3) ~~Violating the relevant security definition requires~~ Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g. AES192)
4) ~~Violating the relevant security definition requires~~ Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384)
~~1)~~5) ~~Violating the relevant security definition requires~~ Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key~~.~~ (e.g. AES 256)

Here, computational resources may be measured using a variety of different metrics (e.g., number of classical elementary operations, quantum circuit size, etc.). In order for a cryptosystem to satisfy one of the above security requirements, any attack must require computational resources comparable to or greater than the stated threshold, with respect to *all* metrics that NIST deems to be potentially relevant to practical security.

NIST intends to consider a variety of possible metrics, reflecting different predictions about the future development of quantum and classical computing technology. NIST will also consider input from the cryptographic community regarding this question.

~~In categorizing submitted parameter sets, NIST will take into account a variety of measures of computational work (e.g. classical security, quantum circuit size at limited depth, combined measures based on the expected cost differential between classical and quantum gates etc.). Which measure is most relevant to practical security will depend on future developments in both classical and quantum computing technology. If plausibly relevant measures yield different categorizations of a parameter set, NIST will generally categorize the parameter set as meeting the lower category.~~

As preliminary guidance to submitters, NIST suggests an approach where quantum attacks are restricted to a fixed running time, or circuit depth. Call this parameter MAXDEPTH. Plausible values for MAXDEPTH range from 2^{40} logical gates (the approximate number of gates that presently envisioned quantum computing architectures [4, 5] are expected to serially perform in a year) through 2^{64} logical gates (the approximate number of gates that current classical computing architectures can perform

Commented [LY(4]: I rewrote what Ray had before, basically to change the emphasis. I want to say that NIST is setting up rules to guide the submitters, rather than making judgements after things have been submitted. I think this is more accurate, and also more diplomatic.

Formatted: Font: Italic

Commented [LY(5]: I copied this from the FAQ, and re-organized it. Note, maybe we can cite refs [4] and [5] in a footnote?

Commented [PR(6]: Someone please check my math on this paragraph. I'm pretty sure it's right, but …

serially in a decade), to 2^{96} logical gates (the approximate number of gates that atomic scale qubits with speed of light propagation times could perform in a millennium).

The complexity of quantum attacks can then be measured in terms of circuit size. These numbers can be compared to the resources required to break AES and SHA3. At the present time, NIST would give the following estimates for the classical and quantum gate counts for the optimal key recovery and collision attacks on AES and SHA3, respectively, where circuit depth is limited to MAXDEPTH.

AES128: 2^{170}/MAXDEPTH quantum gates or 2^{143} classical gates.
SHA3-256: 2^{146} classical gates.
AES192: 2^{233}/MAXDEPTH quantum gates or 2^{207} classical gates.
SHA3-384: 2^{210} classical gates.
AES256: 2^{298}/MAXDEPTH quantum gates or 2^{272} classical gates.
SHA3-512: 2^{274} classical gates.

(Quantum circuit sizes are based on the work in [6]. NIST believes the above estimates are accurate for the majority of values of MAXDEPTH that are relevant to its security analysis, but the above estimates may understate the security of SHA for very small values of MAXDEPTH, and may understate the quantum security of AES for very large values of MAXDEPTH.)

Finally, for attacks that use a combination of classical and quantum computation, one may use a cost metric that rates logical quantum gates as being several orders of magnitude more expensive than classical gates. Presently envisioned quantum computing architectures typically indicate that the cost per quantum gate could be billions or trillions of times the cost per classical gate. However, especially when considering algorithms claiming a high security strength (e.g. equivalent to AES256 or SHA384), it is likely prudent to consider the possibility that this disparity will narrow significantly or even be eliminated.

~~As NIST will be relying heavily on analysis from the cryptographic community, including the submitters, in its evaluations,~~ NIST asks submitters to provide a preliminary classification, according to the above categories, for all parameter sets that they intend to be considered for standardization. All submitters are advised to be somewhat conservative in their preliminary classifications, but submitters of algorithms where the complexity of the best known attack has recently decreased significantly, or is otherwise poorly understood, should be especially conservative.

NIST will not require submitters to provide distinct parameter sets for all five security-strength categories. Submitted parameter sets meeting the requirements of a higher category will be automatically considered to meet the requirements of all lower categories. NIST recommends that submitters provide at least one parameter set that can be provisionally classified as having security strength 4 or 5, and as many additional parameter sets as they feel are appropriate to take advantage of any available security/performance tradeoffs.

Commented [LY(7]: Copied from the FAQ. Cite ref [6] in a footnote?

Commented [MD(8]: Put back in CFP?
Yi-Kai edit here and in 4.A.5

Commented [LY(9R8]: Copied from the FAQ and substantially revised. I left Ray's old version in the FAQ

Commented [LY(10]: Moved up from below

Note that, barring some truly surprising technological development during the standardization process, NIST will assume that the 5 security strengths are correctly ordered in terms of practical security. (E.g., NIST will assume that a brute-force collision attack on SHA256 will be technologically feasible before a brute-force key search attack on AES192.)

Security strengths 1, 3, and 5 are defined in such a way that they are likely to be met by any scheme that:

- Provides classical security strength of 128, 192, and 256 bits, respectively, AND
- Is not subject to quantum attacks, other than classical attacks sped up by generic techniques (Grover's algorithm, quantum walks, amplitude amplification etc.)

Security strengths 1,3, and 5 are unlikely to be met by any scheme with less than 128, 192 or 256 bits of classical security, respectively.

Security strengths 2 and 4 are defined in such a way that they offer the maximum possible quantum security strength that can be offered by a scheme that only has a classical security strength of 128 or 192 bits, respectively. They will generally be easier to meet with parameter sets offering more classical security. A detailed quantum security analysis will be required to determine whether a parameter set meets these security strengths (unless the parameter set also meets the criteria for the next higher security strength).

~~As NIST will be relying heavily on analysis from the cryptographic community, including the submitters, in its evaluations, NIST asks submitters to provide a preliminary classification, according to the above categories, for all parameter sets that they intend to be considered for standardization. All submitters are advised to be somewhat conservative in their preliminary classifications, but submitters of algorithms where the complexity of the best known attack has recently decreased significantly, or is otherwise poorly understood, should be especially conservative.~~

~~NIST will not require submitters to provide distinct parameter sets for all five security strength categories. Submitted parameter sets meeting the requirements of a higher category will be automatically considered to meet the requirements of all lower categories. NIST recommends that submitters provide at least one parameter set that can be provisionally classified as having security strength 4 or 5, and as many additional parameter sets as they feel are appropriate to take advantage of any available security/performance tradeoffs.~~

Commented [LY(11]: Move to FAQ? This sounds more like informal advice to submitters, rather than a formal part of the CFP. Also, if there is disagreement about this, I'd rather have it be in the FAQ, not the CFP.

4.A.6 Additional Security Properties While the previously listed security definitions cover many of the attack scenarios that will be used in the evaluation of the submitted algorithms, there are several other properties that would be desirable:

One such property is perfect forward secrecy[2]. While this property can be obtained through the use of standard encryption and signature functionalities, the cost of doing so may be prohibitive in some cases. In particular, public-key encryption schemes with a slow key generation algorithm, such as RSA, are typically considered unsuitable for perfect forward secrecy. This is a case where there is significant interaction between the cost, and the practical security, of an algorithm.

Another case where security and performance interact is resistance to side-channel attacks. Schemes that can be made resistant to side-channel attack at minimal cost are more desirable than those whose performance is severely hampered by any attempt to resist side-channel attacks. We further note that optimized implementations that address side-channel attacks (e.g., constant-time implementations) are more meaningful than those which do not.

A third desirable property is resistance to multi-key attacks. Ideally an attacker should not gain an advantage by attacking multiple keys at once, whether the attacker's goal is to compromise a single key pair, or to compromise a large number of keys.

A final desirable, although ill-defined, property is resistance to misuse. Schemes should ideally not fail catastrophically due to isolated coding errors, random number generator malfunctions, nonce reuse, keypair reuse (for ephemeral-only encryption/key establishment) etc.

4.A.7 Other Consideration Factors As public-key cryptography tends to contain subtle mathematical structure, it is very important that the mathematical structure be well understood in order to have confidence in the security of a cryptosystem. To assess this, NIST will consider a variety of factors. All other things being equal, simple schemes tend to be better understood than complex ones. Likewise, schemes whose design principles can be related to an established body of relevant research tend to be better understood than schemes that are completely new, or schemes that were designed by repeatedly patching older schemes that were shown vulnerable to cryptanalysis.

NIST will also consider the clarity of the documentation of the scheme and the quality of the analysis provided by the submitter. Clear and thorough analysis will help to develop the quality and maturity of analysis by the wider community. NIST will also consider any security arguments or proofs provided by the submitter. While security proofs are generally based on unproven assumptions, they can often rule out common classes of attacks or relate the security of a new scheme to an older and better studied computational problem.

In addition to NIST's own expectations for the scheme's long-term security, NIST will also consider the judgment and opinions of the broader cryptographic community.

[2] The term *perfect forward secrecy* is commonly used to denote a feature of key agreement protocols which gives assurances that past session keys will not be compromised even if the private key of the server is compromised.

4.B Cost

As the cost of a public-key cryptosystem can be measured on many different dimensions, NIST will continually seek public input regarding which performance metrics and which applications are most important. If there are important applications that require radically different performance tradeoffs, NIST may need to standardize more than one algorithm to meet these diverse needs.

4.B.1 Public Key, Ciphertext, and Signature Size Schemes will be evaluated based on the sizes of the public keys, ciphertexts, and signatures that they produce. All of these may be important consideration factors for bandwidth-constrained applications or in Internet protocols that have a limited packet size. The importance of public-key size may vary depending on the application; if applications can cache public keys, or otherwise avoid transmitting them frequently, the size of the public key may be of lesser importance. In contrast, applications that seek to obtain perfect forward secrecy by transmitting a new public key at the beginning of every session are likely to benefit greatly from algorithms that use relatively small public keys.

4.B.2 Computational Efficiency of Public and Private Key Operations Schemes will also be evaluated based on the computational efficiency of the public key (encryption, encapsulation, and signature verification) and private key (decryption, decapsulation, and signing) operations. The computational cost of these operations will be evaluated both in hardware and software. The computational cost of both public and private key operations is likely to be important for almost all operations, but some applications may be more sensitive to one or the other. For example, signing or decryption operations may be done by a computationally constrained device like a smartcard; or alternatively, a server dealing with a high volume of traffic may need to spend a significant fraction of its computational resources verifying client signatures.

4.B.3 Computational Efficiency of Key Generation Schemes will also be evaluated based on the computational efficiency of their key generation operations, where applicable. As noted in Section 4.A.6, the most common scenario where key generation time is important is when a public-key encryption algorithm or a KEM is used to provide perfect forward secrecy. Nonetheless, it is possible that key generation times may also be important for digital signature schemes in some applications.

4.B.4 Decryption Failures Some public-key encryption algorithms and KEMs, even when correctly implemented, will occasionally produce ciphertexts that cannot be decrypted/decapsulated. For most applications, it is important that such decryption failures be rare or absent. For algorithms with decryption/decapsulation failures, submitters must provide the failure rate, as well as an analysis of the impact on security that these failures could cause. While applications can always obtain an acceptably low decryption failure rate by encrypting the same plaintext multiple times, and interactive protocols can simply restart when key establishment fails, these types of solutions have their own performance costs.

4.C Algorithm and Implementation Characteristics

4.C.1 Flexibility Assuming good overall security and performance, schemes with greater flexibility will meet the needs of more users than less flexible schemes, and therefore, are preferable.

Some examples of "flexibility" may include (but are not limited to) the following:

a. The scheme can be modified to provide additional functionalities that extend beyond the minimum requirements of public-key encryption, KEM, or digital signature (e.g., asynchronous or implicitly authenticated key exchange, etc.).
b. It is straightforward to customize the scheme's parameters to meet a range of security targets and performance goals.
c. The algorithms can be implemented securely and efficiently on a wide variety of platforms, including constrained environments, such as smart cards.
d. Implementations of the algorithms can be parallelized to achieve higher performance.
e. The scheme can be incorporated into existing protocols and applications, requiring as few changes as possible.

4.C.2 Simplicity The submitted scheme will be judged according to its relative design simplicity.

5. Proposed Evaluation Process

NIST will form an internal selection panel composed of NIST employees for the technical evaluations of the submitted algorithms. This panel will analyze the submitted algorithms and review public comments that are received in response to the posting of the "complete and proper" submissions. The panel will also take into account all presentations, discussions and technical papers presented at the PQC standardization conferences, as well as other pertinent papers and presentations made at other cryptographic research conferences and workshops. NIST will issue a report after each PQC standardization conference. Final selections of cryptosystems will be made by NIST and the technical rationale for these decisions will be documented in a final report. The following is an overview of the envisioned submission review process.

5.A Overview

Following the close of the call for submission packages, NIST will review the received packages to determine which are "complete and proper," as described in Sections 2 and 3 of this notice. NIST will post all "complete and proper" submissions at http://www.nist.gov/pqcrypto for public review. To help inform the public, a PQC standardization conference will be held at the start of the public comment process to allow submitters to publicly explain and answer questions regarding their submissions.

The initial phase of evaluation will consist of approximately twelve to eighteen months of public review of the submitted algorithms. During this initial review period, NIST intends to evaluate the submitted algorithms as outlined in Section 5.B. NIST will review the public evaluations of the submitted algorithms' cryptographic strengths and weaknesses, and will use these to narrow the candidate pool for more careful study and analysis. The purpose of this selection process is to identify candidates that are suitable for standardization in the near future. Algorithms that are not included in the narrowed pool may still be considered for standardization at a later date, unless they are explicitly removed from consideration by NIST.

Because of limited resources, and also to avoid moving evaluation targets (i.e., modifying the submitted algorithms undergoing public review), NIST will NOT accept modifications to the submitted algorithms during this initial phase of evaluation.

For informational and planning purposes, near the end of the initial public evaluation process, NIST intends to hold another PQC standardization conference. Its purpose will be to publicly discuss the submitted algorithms, and to provide NIST with information for narrowing the field of algorithms for continued evaluation.

NIST plans to narrow the field of algorithms for further study, based upon its own analysis, public comments, and all other available information. It is envisioned that this narrowing will be done primarily on security, efficiency, and intellectual property considerations. NIST will issue a report describing its findings. Submitters of sufficiently similar algorithms may be asked to merge submissions for the next phase.

Before the start of a second evaluation period, the submitters of the algorithms will have the option of providing updated optimized implementations for use during the next phase of the evaluation. During the course of the initial evaluations, it is conceivable that some small deficiencies may be identified in even some of the most promising submissions. Therefore, for the second round of evaluations, small modifications to the submitted algorithms will be permitted for either security or efficiency purposes. Submitters may submit minor changes (no substantial redesigns), along with a supporting justification that must be received by NIST prior to the beginning of the second evaluation period. (Submitters will be notified by NIST of the exact deadline.) NIST will determine whether the proposed modification would significantly affect the design of the algorithm, requiring a major re-evaluation; if such is the case, the modification will not be accepted. If modifications are submitted, new reference and optimized implementations and written descriptions must also be provided by the announced deadline. This will allow a thorough public review of the modified algorithms during the entire course of the second evaluation phase.

Note: All proposed changes must be conveyed by the submitter; no proposed changes (to the algorithm or implementations) will be accepted from a third party.

The second round of evaluation will consist of approximately twelve to eighteen months of public review, with a focus on a narrowed pool of candidate algorithms. During the

public review, NIST will similarly evaluate these algorithms as outlined in the next section. After the end of the public review period, NIST intends to hold another PQC standardization conference. (The exact date is to be scheduled.)

Following the third PQC standardization conference, NIST will prepare a summary report, which may select algorithm(s) for possible standardization, and/or may determine that a third phase of evaluation is needed. This third evaluation process would be structured similarly to the previous two evaluation periods. Any selected algorithm(s) for standardization will be incorporated into draft standards, which will be made available for public comment.

When evaluating algorithms, NIST will make every effort to obtain public input and will encourage the review of the submitted algorithms by outside organizations. NIST encourages the reviewers to demonstrate their findings and attacks both on the versions with parameters that achieve full security levels, as well as with practical attacks on the provided parameter sets with lower security levels. The final decision as to which (if any) algorithm(s) will be selected for standardization is the responsibility of NIST.

It should be noted that this schedule for the evaluation process is somewhat tentative, depending upon the type, quantity, and quality of the submissions. Specific conference dates and public comment periods will be announced at appropriate times in the future. NIST estimates that some algorithms could be selected for standardization after three to five years. However, due to developments in the field, this could change.

5.B Technical Evaluation

NIST will invite public comments on all "complete and proper" submissions. The analysis done by NIST during the initial phase of evaluation is intended, at a minimum, to include:

i. *Correctness check:* The KAT values included with the submission will be used to test the correctness of the reference and optimized implementations, once they are compiled. (It is more likely that NIST will perform this check of the reference code—and possibly the optimized code as well—even before accepting the submission package as "complete and proper.")

ii. *Efficiency testing:* Using the submitted optimized implementations, NIST intends to perform various computational efficiency tests. This could include, for example, the time required for key generation, encryption, decryption, digital signing, signature verification, or key establishment, as well as the size of keys, ciphertext, and signatures.

iii. *Other testing:* Other features of the submitted algorithms may be examined by NIST.

Platform and Compilers

The above tests will initially be performed by NIST on the *NIST PQC Reference Platform*, an Intel x64 running Windows or Linux and supporting the GCC compiler.

At a minimum, NIST intends to perform an efficiency analysis on the reference platform; however, NIST invites the public to conduct similar tests and compare results on additional platforms (e.g., 8-bit processors, digital signal processors, dedicated CMOS, etc.). NIST may also perform efficiency testing using additional platforms.

NIST welcomes comments regarding the efficiency of the submitted algorithms when implemented in hardware. During the second evaluation period, NIST may request specifications of some of the algorithms using a hardware description language, to compare the estimated hardware efficiency of the submitted algorithms.

Note: If the submitter chooses to submit updated optimized implementations prior to the beginning of the second round of evaluation, then some of the tests performed may be performed again using the new optimized implementations. This will be done to obtain updated measurements.

Note**:** Any changes to the NIST PQC Reference Platform will be noted on http://www.nist.gov/pqcrypto.

5.C Initial Planning for the First PQC Standardization Conference

An open public conference will be held shortly after the end of the submission period, at which the submitters of each "complete and proper" submission package will be invited to publicly discuss and explain their submitted algorithm. The documentation for these algorithms will be made available at the conference. Details of the conference will be 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.

Dated: xxx

Q: Does the requirement for ANSI C source code preclude the use of assembly language optimizations?

A: The optimized code required as part of the submission package should be ANSI C with no assembly (this includes inline assembly). This code is meant to be portable. If significant optimizations can be made with assembly, then it can be included as an additional implementation and discussed in the performance analysis.

Q: Will NIST consider platforms other than the "NIST PQC Reference Platform" when evaluating submissions?

A: The reference platform was defined in order to provide a common and ubiquitous platform to verify the execution of the code provided in the submissions. NIST will include performance metrics from a variety of platforms in our evaluation, including: 64-bit "desktop/server class", 32-bit "mobile class", microcontrollers (32-, 16-, and where possible, 8-bit), as well as hardware platforms (e.g., FPGA). Submitters are encouraged to provide additional implementations for these platforms if possible.

Q: In Sections 4.A.2 and 4.A.4, NIST's CFP sets the number of decryption (resp. signature) queries, that an attacker against a proposed encryption (resp. signature) scheme can make, to at most 2 to the 64. What is the rationale for not letting the adversary make essentially as many queries as the target security?

A) Our reason for primarily considering attacks involving fewer than 2 to the 64 decryption/signature queries is that the number of queries is controlled by the amount of work the honest party is willing to do, which one would expect to be significantly less than the amount of work an attacker is willing to do. Any attack involving more queries than this looks more like a denial of service attack than an impersonation or key recovery attack. Furthermore, effectively protecting against online attacks requiring more than 2 to the 64 queries using NIST standards would require additional protections which are outside the scope of the present postquantum standardization effort, most notably the development of a block cipher with a block size larger than 128 bits. This may be something NIST pursues in the future, but we do not feel it is necessary for addressing the imminent threat of quantum computers. That said, as noted in the proposed call for algorithms, NIST is open to considering attacks involving more queries, and would certainly prefer algorithms that did not fail catastrophically if the attacker exceeds 2 to the 64 queries.

Q: Is the NIST PQC Standardization Process a competition?

A) This process shares many features with NIST competitions, and is modelled after the successes we have had with competitions in the past. There are, however, some important requirements that the current research climate demands we require for this process which constitute significant distinctions between this process and a competition.

First, our handling of the applicants does not coincide with a competition as specified in NISTIR 7977. There will not be a single "winner". Our intention is to select a couple of options for more immediate standardization, as well as to eliminate some submissions as unsuitable. There will likely be some submissions that we do not select for standardization, but that we also do not eliminate and which may be excellent options for a specific application that we're not ready or don't have the contemporaneous resources to standardize. In such a circumstance, we would communicate with the submitters to allow these to remain under a public license for study and practice and to remain under consideration for future standardization. There is no specification for the handling of such an applicant in a competition.

Second, the state of the science in the competitions of the past, i.e. for the AES and SHA-3 competitions, was far more developed than for post-quantum cryptography. Though differences of

opinion are inevitable, the selection of the past winners should not have been too surprising. The situation in post-quantum cryptography is less clear and opinions of required properties are less unanimous. In addition, some of NIST's selection criteria, particularly regarding quantum security, may need further refinement in response to ongoing research.

In many respects, the PQC standardization process is less like a competition, and more like an "analysis of alternatives." The goal of the process is not primarily to pick a winner, but to document the strengths and weaknesses of the different options, and to analyze the possible tradeoffs among them. In the end, even if there is not a final consensus on what constitutes the best option, NIST expects that it will be able to make some selections that most experts will agree are satisfactory. ~~The best we can hope for is to offer selections that most experts can agree are good options, since there will likely be no consensus of what constitutes a best option.~~

Q: Why does NIST's CFP ask submitters to provide a classical security analysis, when the intent is to plan for a world with quantum computers?

A: Classical cryptanalysis is still valuable for a number of reasons. First, classical computers are not going away. For algorithms not subject to dramatic quantum attacks, such as those involving Shor's algorithm, NIST believes that classical measures of security will continue to be highly relevant. Currently envisioned quantum computing technologies would be orders of magnitude slower and more energy intensive than today's classical computing technology, when performing the same sorts of operations. In addition, practical attacks typically must be run in parallel on large clusters of machines, which diminishes the speedup that can be achieved using Grover's algorithm. ~~When these considerations are combined with the poor parallelization of Grover's algorithm,~~ When all of these considerations are taken into account, it becomes quite likely that variants of Grover's algorithm will provide no advantage to an adversary wishing to perform a cryptanalytic attack that can be completed in a matter of years, or even decades. As most quantum attacks on proposed postquantum cryptosystems have involved some variant of Grover's algorithm, it may be the case that the best attack in practice will simply be the classical attack.

Also, the science involved in assessing classical security is better developed than that for assessing quantum security, and there is a larger community of researchers who can contribute to these investigations, increasing our confidence in the security of the proposed cryptosystems. Finally, classical cryptanalysis can improve our understanding of the mathematical structures underlying these cryptosystems, which is also the basis for quantum cryptanalysis.

~~Additionally, even if the classical attack does not prove to be the most practical attack in the future, the best classical attack will often be highly predictive of the complexity of the best quantum attack (provided there is no dramatic quantum speedup similar to Shor's algorithm.) At present, the science involved in assessing classical security is better developed than that for assessing quantum security.~~

Q: How does NIST plan to measure the complexity of attacks involving quantum computers? ~~Does NIST feel that existing measures of quantum security that appear in academic literature are adequate?~~How does this differ from previous estimates that have appeared elsewhere?

A: Existing measures of quantum security will often ignore the very real challenges involved in implementing a quantum attack. Most notably they ignore the difficulties involved in parallelizing quantum algorithms, and the fact that quantum gates are expected to be much slower and more expensive than classical gates. This leads to claims, for example, that an algorithm with a 128 bits of classical security and no known quantum speedup, should be considered just as secure as a 256-bit block cipher

Formatted: Indent: First line: 0.5"

Commented [Office1]: We want to mention that the criteria/timeline could change as well, due to the uncertainties in the field.

Add analysis of alternatives

Commented [LY(2R1]: Done

Commented [MD(3]: Yi Kai will add some things to this

Commented [LY(4R3]: Done

like AES256, since both have "128 bits of quantum security". NIST strongly disagrees with this analysis and can think of no realistic model of future computing technology where this is likely to be the case. The requirement that submitters provide classical security analysis, and that their parameter sets be categorized in a way that takes classical security into account, mitigates this problem somewhat, but it does not completely eliminate it. In addition to classical attacks, an algorithm may be susceptible to quantum attacks that either parallelize well, or can be made inexpensive by performing a significant portion of the necessary computation classically. NIST feels its categorization of the security such schemes should reflect these threats.

While NIST will continue throughout the evaluation process to accept input from the cryptographic community regarding the best way to measure quantum security, so that it is likely to reflect the real world cost of attacking a scheme, NIST currently favors an approach where quantum attacks are given a strict maximum bound on depth, and then measured based on circuit size. Such attacks may also have a cost metric that rates logical quantum gates as being several orders of magnitude more expensive than classical gates.

Plausible limitations on depth range from 2^{40} logical gates (the approximate number of gates that presently envisioned quantum computing architectures [4, 5] are expected to serially perform in a year) through 2^{64} logical gates (the approximate number of gates that current classical computing architectures can perform serially in a decade), to 2^{96} logical gates (the approximate number of gates that atomic scale qubits with speed of light propagation times could perform in a millennium). Presently envisioned quantum computing architectures typically indicate that the cost per quantum gate could be billions or trillions of times the cost per classical gate. However, especially when considering algorithms claiming a high security strength (e.g. equivalent to AES256 or SHA384), it is likely prudent to consider the possibility that this disparity will narrow significantly or even be eliminated.

Q: In section 4.A.5 of its CFP, NIST defines security strength categories for submitted algorithms in terms of the security of its existing standards in symmetric cryptography. Can NIST quantify the security of these standards?

A: At the present time, NIST would give the following estimates for the classical and quantum gate counts for the optimal key recovery and collision attacks on AES and SHA3, respectively, where circuit depth is limited to MAXDEPTH.

AES128: 2^{170}/MAXDEPTH quantum gates or 2^{143} classical gates.
SHA3-256: 2^{146} classical gates.
AES192: 2^{233}/MAXDEPTH quantum gates or 2^{207} classical gates.
SHA3-384: 2^{210} classical gates.
AES256: 2^{298}/MAXDEPTH quantum gates or 2^{272} classical gates.
SHA3-512: 2^{274} classical gates.

(Quantum circuit sizes are based on the work in [6]. NIST believes the above estimates are accurate for the majority of values of MAXDEPTH that are relevant to its security analysis, but the above estimates may understate the security of SHA for very small values of MAXDEPTH, and may understate the quantum security of AES for very large values of MAXDEPTH.)

Commented [LY(5]: NIST is getting pretty worked up about this point! Maybe revise this so it comes across as more informative and less opinionated?

Commented [MD(6]: Put back in CFP?
Yi-Kai edit here and in 4.A.5

Commented [PR(7]: Someone please check my math on this paragraph. I'm pretty sure it's right, but …

Q: In section 4.A.5, it is stated that NIST will assume that its 5 security categories are correctly ordered (i.e. that a collision attack on SHA256 (resp. SHA384) will be harder to perform than a key search attack on AES192 (resp. AES 256.)) How realistic is this assumption?

A: Even assuming no disparity in the cost of quantum and classical gates, the assumption holds as long as the adversary is depth limited to fewer than about 2^{87} logical quantum gates. This is quite near the limit of what NIST considers to be a plausible technology for the foreseeable future.

Commented [MD(8]: Check this is okay with Sara

[4] N. C. Jones, R. Van Meter, A. G. Fowler, P. L. McMahon, J. Kim, T. D. Ladd, and Y. Yamamoto, Layered Architecture for Quantum Computing, Phys. Rev. X 2, 031007 (2012) http://journals.aps.org/prx/pdf/10.1103/PhysRevX.2.031007

[5] M. Mariantoni, Building a Superconducting Quantum Computer, Invited Talk PQCrypto 2014, October 2014 Waterloo, Canada. https://www.youtube.com/watch?v=wWHAs--HA1c [accessed 10/24/2016]

[6] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, Applying Grover's algorithm to AES: quantum resource estimates, in T. Takagi, editor, Post-Quantum Cryptography, Lect. Notes in Comput. Sci. vol. 9606, Springer, pp. 9–43 (2016) http://link.springer.com/chapter/10.1007%2F978-3-319-29360-8_3