From: David A. Cooper
To: Barker, Elaine B. (Fed); Sonmez Turan, Meltem (Fed); Moody, Dustin (Fed); Chang, Shu-jen H. (Fed); Kelsey, John M. (Fed); Dworkin, Morris J. (Fed); McKay, Kerry A. (Fed); Dang, Quynh H. (Fed); Bill Burr (b) (6) Regenscheid, Andrew R. (Fed)
Cc: Liu, Yi-Kai (Fed); Chen, Lily (Fed); Perlner, Ray A. (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Jordan, Stephen P (Fed); Peralta, Rene C. (Fed); Bassham, Lawrence E. (Fed)
Subject: Re: Post-Quantum Crypto - Call For Submissions - comments requested
Date: Friday, April 29, 2016 1:38:57 PM
Attachments: DC ebb-Meltem-sj Post QuantumCFP v8.docx

Attached are my comments added to Elaine's, Meltem's, and Shu-jen's.

Dave

On 4/29/16 11:20 AM, Barker, Elaine B. (Fed) wrote:

> I added my comments to Meltem's and Shu-jen's.
>
> Elaine
>
> **From:** Meltem Turan <meltem.turan@nist.gov>
> **Date:** Wednesday, April 20, 2016 at 11:32 AM
> **To:** "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Barker, Elaine B." <elaine.barker@nist.gov>, Shu-jen <shu-jen.chang@nist.gov>, John Kelsey <john.kelsey@nist.gov>, Morris Dworkin <morris.dworkin@nist.gov>, "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>, Quynh <quynh.dang@nist.gov>, David Cooper <david.cooper@nist.gov>, "Bill Burr (home)" (b) (6) Andrew <andrew.regenscheid@nist.gov>
> **Cc:** "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Chen, Lily" <lily.chen@nist.gov>, Ray Perlner <ray.perlner@nist.gov>, "Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)" <daniel-c.smith@louisville.edu>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "'rene. gov'" <rene.peralta@nist.gov>, Larry Bassham <lawrence.bassham@nist.gov>
> **Subject:** RE: Post-Quantum Crypto - Call For Submissions - comments requested
>
> Hi everyone,
> I attached my comments on the call for submissions.
> Meltem
>
> **From:** Moody, Dustin (Fed)
> **Sent:** Monday, April 18, 2016 12:35 PM
> **To:** Barker, Elaine B. (Fed) <elaine.barker@nist.gov>; Chang, Shu-jen H. (Fed) <shu-jen.chang@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Dang, Quynh (Fed) <quynh.dang@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>; Bill Burr (b) (6) Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>

Cc: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu) <daniel-c.smith@louisville.edu>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Subject: Post-Quantum Crypto - Call For Submissions - comments requested
Everyone,

As you hopefully know, we are going to be calling for submissions for quantum-resistant algorithms to replace the current public-key algorithms in our standards. Our PQC team has written the attached Call for submissions, which we plan to release for public comments shortly. We've edited it pretty extensively in our group, but would like some more eyes to take a look, since this will be a pretty big undertaking.

Can you all please review the Call, and submit comments back by Friday, April 29th? We would greatly appreciate it. Any questions, just let me know. Thanks!

Dustin

Billing Code:

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.:

Announcing Request for Proposals for Quantum-Resistant Cryptographic Algorithms

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice and request for nominations for candidate Quantum-Resistant Cryptographic Algorithms.

SUMMARY: This notice solicits nominations from any interested party for candidate quantum-resistant cryptographic algorithms to be considered for new standards for key establishment, public-~~–~~key encryption and digital signatures that will be secure against quantum computation. It addresses the nomination requirements and the minimum acceptability requirements of a ~~‘‘~~“complete and proper”~~’’~~ submission. The evaluation criteria that will be used to appraise the submitted algorithms are also described.

Commented [STM(1]: Throughout the document, replace ‘‘ with “.

DATES: Submission packages must be received by DATE. Further details are available in Section 2.

ADDRESSES: Submission packages should be sent to: XXX, Information Technology Laboratory, Attention: Quantum-Resistant Cryptographic Algorithm Submissions, 100 Bureau Drive – Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930.

FOR FURTHER INFORMATION CONTACT: For general information, send e-mail to pqc-comments@nist.gov. For questions related to a specific submission package, contact XXX, National Institute of Standards and Technology, 100 Bureau Drive – Stop 8930, Gaithersburg, MD 20899–8930; telephone: +1 301–975–XXX or via fax at +1 301–975–8670, e-mail: XXX@nist.gov.

Commented [STM(2]: Do we need 2.F? it also provides this email address.

SUPPLEMENTARY INFORMATION: This notice contains the following ~~section~~sections:

Commented [STM(3]: How about the numbering format 1.1.1., rather than 1.A.1??

Commented [BEB4]: not defined yet

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 ~~exchange,~~establishment and play a crucial role in ensuring the confidentiality and authenticity of communications on the Internet and other networks.

Commented [BEB5]: Change to establishment! This is even use below

Due to this concern, many researchers have begun to investigate post-quantum cryptography (PQC) (also called quantum-resistant 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~~,~~ in the event that large-scale quantum computers become a reality.

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

Commented [SC6]: I probably won't call these "candidates" yet, since they have not been submitted for consideration.

Formatted: Strikethrough

Formatted: Strikethrough

Commented [BEB7]: what is a quantum adversary? Do you mean adversaries with quantum capabilities?

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 painless, 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 algorithms. In addition, this transition needs to take place well before any large-scale quantum computers are built, so that any information ~~which~~ 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 taking a number of steps with regard to standardizing post-quantum cryptography. First, as an interim solution, NIST allows the use of "hybrid modes," which combine a currently approved cryptographic algorithm with a post-quantum algorithm, in such a way that the combined system is at least as secure as the stronger of the two components. Such hybrid modes can be approved for use under existing NIST guidelines. In addition, NIST will work to ensure appropriate coordination with other standardization efforts (for instance, efforts to standardize stateful hash-based signatures).

Most importantly, NIST is beginning a process to develop new post-quantum standards for key establishment, public-~~-~~key encryption, and digital signatures. In developing these standards, NIST has two main considerations. First, these cryptosystems should provide strong security against both classical and quantum computers (and combinations thereof). Second, these cryptosystems should be easy to deploy in existing applications and protocols, such as Transport Layer Security (TLS), Internet Key Exchange (IKE), and digital certificates. In particular, these cryptosystems will be used to replace existing NIST standards that are not secure against quantum computers, including Federal Information Processing Standards Publication (FIPS) 186, the *Digital Signature Standard (DSS)*, and NIST Special Publications (SP) 800-56 A/B, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* and *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*.

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

NIST is soliciting proposals for post-quantum cryptosystems from the community, and it will solicit comments from the ~~community~~ public as part of its evaluation process. NIST expects to perform multiple rounds of evaluation, over a period of three~~3~~ to ~~-~~five~~5~~ years. The goal of this process is ~~will be~~ to select some number of acceptable candidate cryptosystems~~, which~~ that will then be developed into NIST standards.

Commented [STM(8]: Which community ? Can we add 'crypto" or academic here?

SJ – How about "any interested party" as stated in the SUMMARY Section?

Commented [SC9]: I use this word because we will be soliciting "public comments".

Commented [SC10]: You can simplify this statement by "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. A final reason is that some of the candidate cryptosystems may have completely different design attributes and mathematical foundations, so that a direct comparison is simply impossible.

As a result of these complexities, NIST believes that the post-quantum standards development process should not be treated as a competition. Due to the uncertainties in the evaluation of the submissions, in some cases, it may not be possible to make a well-supported ~~judgement~~judgment that one candidate is “better” than another. Rather, the goal of the process is to perform a thorough analysis of the submitted algorithms~~,~~ in a manner ~~which~~ that is open and transparent to the~~-~~ public~~community~~. This will inform NIST’s decision on the subsequent development of post-quantum standards.

2. Requirements for the Submission Packages

Submission packages must be received by NIST by XXX. Submission packages received before XXX will be reviewed for completeness by NIST; the submitters will be notified of any deficiencies by XXX, allowing time for deficient packages to be amended by the submission deadline. No amendments to packages will be permitted after the submission deadline.

Due to the specific requirements of the submission package such as Intellectual Property Statements / Agreements / Disclosures as specified in ~~s~~Section 2.D, e-mail submissions will not be accepted for these statements or for the initial submission package. However, e-mail submissions of amendments to the initial submission package will be allowed prior to the submission deadline.

“~~‘‘~~Complete and proper”~~’’~~ submission packages received in response to this notice will be posted at http://csrc.nist.gov/groups/ST/post-quantum-crypto/ -for ~~inspection~~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.~~Each of these items is discussed in detail below.~~

2.A Cover Sheet

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

Commented [BEB11]: How about "quantum-resistant" here?

Commented [STM(12]: How about “direct comparison of candidates”?

EBB: How about :"direct comparison with classical cryptosystems"?

Commented [SC13]: I’m not sure this is the right word to use here. How about “convey”, “explain”, or “substantiate”?

EBB: "support" or "facilitate" might also work here

Commented [DC14]: This part confuses me. Two paragraphs above it says that “The goal of this process is to select some number of acceptable cryptosystems, which will then be developed into NIST standards.” Are these two paragraphs trying to say different things? I thought one big difference between this process and the SHA-3/AES process was that we didn’t expect to find one algorithm that would be well suited to all use cases (e.g., an algorithm that is good for code signing may not work well for performing authentication from a PIV Card).

Commented [MD(15]: Two months before the deadline

Commented [MD(16]: One month before the deadline

Commented [BEB17]: Do we really want to say this? If someone comes up with something really outstanding, do we want to refuse it? This is not a competition, but a world-wide effort to deal with an upcoming situation.

Commented [STM(18]: Throughout the document, Sections should be capitalized.

Commented [STM(19]: We haven’t defined what we mean by ‘proper’ yet.

Commented [MD(20]: Might be updated to www.nist.gov/pqcrypto

- Name of the proposed cryptosystem.
- Principal submitter's name, e-mail address, telephone, fax, 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 shall 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; and 6) a statement of advantages and limitations.

Commented [BEB21]: How about "must"? Consider this instead of "shall" throughout this announcement.

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, diagrams, and parameters that are needed to implement the algorithms. The document shall include design rationale and an explanation for all the important design decisions that ~~are~~ 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 establishment, and digital signatures. Public-key encryption schemes shall include algorithms for key generation, encryption, and decryption. Key-establishment schemes shall include algorithms for generating initiator and responder key-~~exchange~~ establishment messages, as well as algorithms for both initiator and responder to recover a shared secret. Digital-signature schemes shall include algorithms for key generation, signature generation~~,~~ and signature verification.

Commented [BEB22]: Does the term "public key encryption" refer to general data that could be very long, or is it being used to address the encryption of keys, as in RSA key transport?

Is the term "key establishment" referring to key agreement, in which case the use of initiator and responder is appropriate (as in 56A and 56B), or is it also including key transport, in which case the use of sender and receiver is appropriate.?

Commented [STM(23]: Formal mathematical definitions of these algorithms might be helpful.

In addition, the submission shall specify several parameter sets ~~which~~ that allow the selection of a range of possible security/performance tradeoffs, as well as the construction of weakened versions of the submitted algorithm for analysis. In particular, the submitter shall provide an analysis of how the security and performance of the algorithm depend on these parameter sets. 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 if it plans to select that algorithm for standardization, but with a different parameter set than originally specified by the submitter.

Commented [STM(24]: How about academic community? Shall we ask for public comment, if we plan to modify the algorithm?

EBB: I think it should be more than the submitter or academic community. Cryptographic community?

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 ~~nonstandard~~ cryptographic primitive that has not been approved by NIST, the submitter shall provide an explanation for why a ~~standard~~ NIST-approved primitive would not be suitable.

If a compatibility construct is needed in order to provide a drop-in replacement for the algorithms and schemes specified in FIPS or NIST Special Publications, this construct must be described. If the submitted algorithms cannot be used as a drop-in replacement for the schemes specified in FIPS or NIST Special Publications, the point(s) of failure must be clearly indicated.

To prevent the existence of possible ‘‘trap-doors’’ in an algorithm, the submitter shall explain the provenance of any constants or tables used in the algorithm.

Commented [STM(25]: What is considered to be acceptable ? What is not?

2.B.2 Also to be included is a statement of the algorithms’ estimated computational efficiency and memory requirements for the ‘‘NIST PQC Reference Platform’’ (specified in ~~s~~Section 5.B). Efficiency estimates for other platforms may be included at the submitters’ discretion. These estimates shall each include the following information, at a minimum:

a. ~~Description~~ 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 (e.g., for software running on a PC, include information about the processor, clock speed, memory, operating system, etc.). For hardware estimates, a gate count (or estimated gate count) should be included.

Commented [BEB26]: define/spell out. Why even say "running on a PC?

Commented [STM(27]: In SPs we are very careful with how we state requirements. Here we sometimes use “shall”, “should” “must” etc.

EBB: I would think that must and should would be OK in this document

b. ~~Speed~~ A speed estimate and memory requirements for the algorithm(s) on the reference platform specified in ~~section~~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).

Commented [SC28]: I’m not familiar with PQC, so I can’t comment on the relevance of these requirements for a PQC algorithm, but I do wonder about that, and like to share this thought with you.

This comment may also apply to the other requirements addressed below.

2.B.3 In addition, each submission package is required to include Known Answer Test (KAT) values~~, which~~ 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 ~~is randomized~~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 exercise 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 or DVD as described in ~~section~~Section 2.C.4.

Each file shall be clearly labeled with header information listing:

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

~~Followed~~ The list must be followed by a set of tuples where all values within the tuple ~~shall be~~is clearly labeled (*e.g.*, Plaintext, PublicKey, RandomBits, Ciphertext, etc.). Sample files for these KAT values will be posted at http://csrc.nist.gov/groups/ST/post-quantum-crypto/.

Commented [SC29]: This sentence doesn't parse; it seems to be missing some phrase.

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

i. ~~-~~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*.

Commented [BEB30]: why is there a shift to roman numerals (i and ii)?

ii. If tables are used in an algorithm, then a set of KAT vectors shall be included to exercise every table entry.

Note: The submitter is encouraged to include any other KATs that exercise 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.

Commented [SC31]: See my previous comment about requirement relevance. This example may be fine, I just like you to be sure.

2.B.4 The submission package shall include a statement of the expected security strength of the cryptosystem, along with a supporting rationale. This statement shall include a description of which of the parameter settings~~, specified by the submitter,~~ that the submitter is confident ~~to~~will meet or exceed each of the security targets specified in ~~section~~Section 4.A.4, for at least one of the security models specified in ~~section~~Sections 4.A.2 and ~~section~~ 4.A.3. If the submitter believes that these settings exceed the relevant security target, the submitter shall give an estimate of how much the settings will exceed the security target. Furthermore, ~~Additionally,~~ the statement should address ~~discuss~~ the additional attack scenarios identified ~~specified~~ in ~~section~~Section 4.A.5.

2.B.5 The submission package shall include a statement that summarizes the known cryptanalytic attacks on this~~e~~ 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. 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.

Commented [BEB32]: was this a requirement above? here, it sounds like this is optional.

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.

In addition, this statement may also 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 ~~H~~hardware ~~D~~description ~~L~~language (HDL).

Commented [BEB33]: or cryptosystem?

2.C Optical Media

All electronic data shall be provided on a single CD-ROM or DVD 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 ~~programming~~ is more important than the efficiency of the code. The reference implementation should include appropriate comments and clearly map the implementation code to the algorithm description included in ~~section~~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 ~~candidate~~ proposed algorithm. This includes support for all core features of the algorithm, e.g., key generation, public ~~-~~key validation, and digital signature generation~~,~~ ~~digital~~and ~~signature~~ verification~~validation~~.

A separate document specifying a set of cryptographic service calls, namely a cryptographic API, for the ANSI C implementations, will be made available at http://csrc.nist.gov/groups/ST/post-quantum-crypto/. 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.

Commented [DC34]: Removed all the "\" since they are Microsoft-specific and aren't needed.

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 on the CD–ROM or DVD shall contain all of the required test values as specified in ~~required under section~~Section 2.B.3~~ of this announcement~~.~~. That section includes descriptions of the required tests, as well as a list of the values that must be provided.~~

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 ~~an~~ 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 appropriate links within the PDF~~ as appropriate~~.

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

2.C.4 General Requirements for Optical Media For the portions of the submission that may be provided electronically, the information shall be provided on a single CD-ROM or DVD using the ISO 9660 format. This disc shall have the following structure:

- ~~\~~README
- ~~\~~Reference_Implementation
- ~~\~~Optimized_Implementation
- ~~\~~KAT
- ~~\~~Supporting_Documentation

The "README" file shall list all files that are included on this disc with a brief description of each.

Commented [DC35]: Format? Plain text, HTML

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 ~~re-~~submitted.

2.D Intellectual Property Statements / Agreements / Disclosures

Each submitted algorithm must be available worldwide on a royalty free basis during the period of the quantum-resistant algorithm search. In order to ensure this and minimize any intellectual property issues, the following series of signed statements are required for a submission to be considered complete: 1) ~~S~~statement by the ~~S~~submitter, 2) ~~S~~statement by ~~P~~patent (and ~~P~~patent ~~A~~application) ~~O~~owner(s) (if applicable), and 3) ~~S~~statement by ~~R~~reference/~~O~~optimized ~~I~~implementations' ~~O~~owner(s). Note that for the last two statements, separate statements must be completed if multiple individuals are involved.

Commented [BEB36]: As worded, this seems to imply that afterwards, intellectual property rights resume?

2.D.1 Statement by the Submitter

I, _____ (print submitter's full name) do hereby declare that, to the best of my knowledge, the practice of the cryptosystem, reference implementation, and 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 appropriate)_____ .

Commented [STM(37]: This line is not needed.

I do hereby declare that I am aware of no patent applications that may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations. – **OR** *– I do hereby declare that the following pending patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate) ______.*

I do hereby understand that my submitted cryptosystem might not be selected for standardization by NIST. I further understand that I will not receive financial 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 relating to my cryptosystem. I also understand that the U.S. Government may, during the course of the lifetime of the standard or during the public review process, modify the cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I understand that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment. Should my submission be selected for standardization, I hereby agree not to place any restrictions on the use of the cryptosystem, intending it to be available on a worldwide, non-exclusive, royalty-free basis.

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 evaluation process.

I understand that, during the quantum-resistant 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 the submitter, I understand that all rights, including use rights of the reference and optimized implementations, revert back to the submitter (and other owner(s), as appropriate).

Signed:

Commented [STM(38]: Signature ?

Title:
Dated:
Place:

Commented [STM(39]: Is this needed?

Commented [STM(40]: Date ?

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 of the patent and patent applications above 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 agree to grant to any interested party if the cryptosystem known as _____(print name of cryptosystem) ________is selected for standardization, an irrevocable nonexclusive royalty-free license to practice the referenced cryptosystem, reference implementation or the optimized implementations. Furthermore, I agree to grant the same rights in any other patent application or patent granted to me or my company that may be necessary for the practice of the referenced cryptosystem, reference implementation, or the optimized implementations.

Signed:
Title:
Dated:
Place:

Note that the U.S. government may conduct research as may be appropriate to verify the availability of the submission on a royalty free basis worldwide.

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

The following must also be included:

I, _____ (print full name) ______, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to use such implementations for the purposes of the quantum-resistant algorithm evaluation process, notwithstanding that the implementations may be copyrighted.

Signed:
Title:
Dated:
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 submitted in a language other than English shall render the submission package ‘‘incomplete.’’ Optional supporting materials (e.g., journal articles) in another language may be submitted.

Commented [BEB41]: How about "{not submitted in English", since there's nothing wrong with submitting the information in multiple languages?

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 Lily Chen, National Institute of Standards and Technology, 100 Bureau Drive—Stop 8930, Gaithersburg, MD 20899–8930; telephone: +1 301–975–6974 or via fax at +1 301–975–8670, e-mail: lily.chen@nist.gov.

Answers to germane questions will be posted at http://csrc.nist.gov/groups/ST/post-quantum-crypto/. 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. Minimum Acceptability Requirements

Those submission packages that are deemed 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 available worldwide without royalties or any intellectual property restrictions.
2. The algorithms shall not incorporate major components that are ~~not~~ 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 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.

Commented [DC42]: Did you mean to only accept those are already believed to be secure against quantum computers, or did you just want to exclude those that are already believed to be insecure? I assumed the latter, with it being the responsibility of the submitter to convince reviewers that their proposal is secure.

Commented [BEB43]: See my comment above about the intent of these terms

Commented [BEB44]: Is relayive long messages implied here?

Commented [STM(45]: Do we want to say security level instead?

EBB: no. I think length is meant here.

Commented [BEB46]: Is this intended to be a replacement for RSA-=like key transport?

b. Key-exchange schemes shall include algorithms for generating initiator and responder key-exchange messages, as well as algorithms for both initiator and responder to recover a shared secret. Initiators and responders conforming to the specified algorithms shall recover the same secret with high probability. If failed key establishment is a possibility, it shall occur at a rate consistent with claims made by the submitter. At a minimum, the key-exchange functionality shall support the establishment of shared keys of length at least 256 bits.

Commented [STM(47]: Do we have a requirement on this probability ?

Commented [BEB48]: Exchange is the wrong word. This definition seems to be implying key agreement, which is a subcategory of key-establishment.

We should be using terms that are consistent with 56A and 56B.

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 meet or exceed (to the best of the submitter's knowledge) the relevant security targets in ~~section~~Section 4.A.4, for the appropriate security models in ~~section~~Sections 4.A.2 and 4.A.3.

Commented [SC49]: I think the purpose of this section, as stated, is very different from that of the SHA-3 competition. If this is what you intended, it's fine.

For the SHA-3 competition, the purpose of Sec. 3 was to allow us to be able to determine quickly whether a submission merits a close look. So the minimum acceptability requirements were something easy to assess, not something that require time to analyze. I feel what you have listed here may be more involved than necessary.

A submission package that is complete (as defined in ~~section~~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 is deemed otherwise at the close of the submission period will receive no further consideration. Submissions that are ‘‘complete and proper'' will be posted at http://csrc.nist.gov/groups/ST/post-quantum-crypto/ for public review.

4. 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~~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.

Commented [STM(50]: This might need more explanation. What is really suggested here? Submitters to announce their intent publicly before submission?

If there are submissions based on similar cryptosystems, how will NIST respond ?

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 quantum-resistant 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 I~~i~~nternet protocols, such as TLS, SSH, IP~~S~~sec, and DNSSEC~~sec~~. 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.

Commented [BEB51]: This is why the terms above need to be consistent with the terms used in 56A and B. I can help, if you'd like.

4.A.2 Security Model for Encryption/Key-Establishment One particularly important application of public-key cryptography is key transport (i.e., public-key encryption of a symmetric key). NIST intends to standardize at least one scheme ~~which~~ that enables "semantically secure encryption" with respect to adaptive chosen ciphertext attack. (This property is generally denoted *IND-CCA2 security* in academic literature.)

Commented [SC52]: If the CFS needs to be approved by the NIST lawyers before being published, I suspect they will ask about this term.

Formatted: Font: Italic

The above security model should be taken as a statement of what NIST will consider to be a relevant attack. Submitted schemes for encryption and key exchange 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.

Commented [BEB53]: key establishment? key ageement?

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 ~~which~~ that use classical (rather than quantum) queries to the decryption oracle or other private-key functionality.

4.A.3 Security Model for Digital Signatures NIST intends to standardize at least one scheme ~~which~~ that enables existentially unforgeable digital signatures with respect to an adaptive chosen message attack. (This property is generally denoted *EUF-CMA security* in academic literature.)

Formatted: Font: Italic

The above security model 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 level~~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 ~~which~~ that use classical (rather than quantum) queries to the signing oracle.

4.A.4 Target Security Strength~~Level~~s Submitters are asked to provide parameter sets that meet or exceed each of five target ~~security level~~security strengths:

1) 128 bits classical security / 64 bits quantum security

2) 128 bits classical security / 80 bits quantum security
3) 192 bits classical security / 96 bits quantum security
4) 192 bits classical security / 128 bits quantum security
5) 256 bits classical security / 128 bits quantum security

In specifying these ~~security level~~security strengths, the intent is that parameter sets meeting ~~security level~~security strengths 1, 3, and 5 will remain secure as long as brute-force attacks against AES-~~–~~128, AES-~~–~~192, and AES-~~–~~256, respectively, remain infeasible. Likewise, parameter sets meeting ~~security level~~security strengths 2 and 4 should remain secure, roughly as long as brute-force collision attacks against SHA-~~–~~256/ SHA3-256 and SHA-~~–~~384/SHA3-384, respectively, remain infeasible.

Some care is needed to precisely define the meaning of these ~~security level~~security strengths. Intuitively, k bits of classical security means that the best cryptanalytic attack requires 2^k classical computing resources, and k bits of quantum security means that the best cryptanalytic attack requires 2^k quantum computing resources. To make this statement precise, however, one must choose an appropriate unit of computational "work." To resolve this ambiguity, NIST proposes to *define* the units of computational work to be such that AES-128 has 128 bits of classical security and 64 bits of quantum security. This is plausible under the assumption that there are no attacks on AES that require ~~are~~ significantly less work ~~cheaper~~ than a~~the~~ brute-~~–~~force search.

NIST will also consider other factors ~~which~~ that affect the feasibility of an attack, such as how easily the attack can be parallelized, and whether the attack can be implemented using special-purpose hardware (such as hybrid quantum-classical architectures, quantum annealers, graphics processing units, neuromorphic architectures, and others). NIST also recognizes that there is some uncertainty regarding the best way to measure the practical feasibility of cryptanalytic attacks, especially attacks using quantum computers.

Parallelizability of attacks is a major concern for NIST. NIST is concerned with the most practical attack on a cryptosystem, which may not be the one requiring the smallest number of operations. In particular, an attack requiring a larger total number of operations may be more practical than one ~~which~~ that requires fewer operations~~,~~ if the former is more amenable to speedup via parallel execution (i.e., reducing its time complexity by performing more computations in parallel).

One of the simplest examples of this phenomenon involves hash functions: A quantum preimage attack on a 2*s*-bit hash function, using Grover's algorithm, has roughly the same complexity as a classical search for collisions on the same 2*s*-bit hash function (ignoring costs associated with reversibility, fault tolerance, etc.). However, Grover's algorithm parallelizes significantly more poorly than classical collision search. As a result, in a~~the~~ realistic scenario where the attacker performs many operations in parallel, classical search for collisions on a 2*s*-bit hash has a significantly lower time complexity than quantum preimage search on the same hash function.

Commented [BEB54]: should s be defined (e.g., the claimed security strength for collision resistance)?

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Since NIST's goal is that schemes with parameters assigned *s* bits of quantum security be strictly harder to break than a block cipher with a 2*s*-bit key, NIST will generally assign less than *s* bits of quantum security~~,~~ if, as in the case of classical collision search, there is a parallel attack (classical or quantum) ~~which~~ that has lower time complexity than an equivalently-parallel quantum attack on a block cipher with a 2*s*-bit key. Ideally, the submitted parameter sets should meet or exceed the quantum security of a block cipher with a 2*s*-bit key for any degree of parallelism, but NIST recognizes that extremely serial or extremely parallel attacks (e.g., those that have a time depth or space complexity exceeding 2^{100}) may be of minimal practical importance.

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Finally, NIST will consider the extent to which attacks can be made less expensive by doing some or all of the computation on hardware (e.g., classical computing hardware) that may be less expensive to produce or maintain than general purpose quantum computing hardware. It is not, however, clear how difficult it will be~~is~~ to build large-scale quantum computers. It appears that quantum computations will be significantly more expensive to perform than classical computations~~,~~ using current and near-future technologies, due to the need for quantum error correction and distinctive hardware requirements, such as extreme cooling. Nevertheless, it is difficult to predict how these technologies will develop, or whether quantum computers will ever scale in a way that is analogous to "Moore's law" for semiconductor-based classical computers.

For the purpose of developing post-quantum cryptosystems, it may be prudent to plan for the extreme scenario where quantum computers will be~~are~~ relatively cheap and ubiquitous. NIST will therefore take quantum attacks seriously, even if they require the full power of a general purpose quantum computer.

4.A.5 Additional Security Properties While the previously listed security definitions cover many of the attack scenarios ~~which~~ that will be used in the evaluation of the submitted algorithms, there are several other properties ~~which~~ that would be desirable:

One such property~~,~~ is perfect forward secrecy. 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.

Commented [SC55]: Is this the right word to use here? Are you thinking about "tradeoff"?

Another case where security and performance interact is resistance to side-channel attack. Schemes ~~which~~ 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.

Commented [SC56]: See my comment above. It's ok if you can't find a better word to use for this.

A third desirable property is resistance to multi-key attacks. Ideally an attacker should not gain any 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, etc.

4.A.6 Other Consideration Factors ~~-~~As public-~~-~~key cryptography tends to contain subtle mathematical structure, it is very important that ~~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 cryptographic research tend to be better understood than schemes that are completely new, or schemes that were designed by repeatedly patching older schemes ~~which ~~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 ~~long-term security, NIST will also consider the ~~judgement~~judgment and opinions of the broader cryptographic community.

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 ~~which ~~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~~Internet protocols that have a limited packet size. The importance of public-~~-~~key size may vary depending on the application;~~: I~~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 and signature verification) and private key (decryption 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 (e.g.,, 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~~Section 4.A.5, the most common scenario where key generation time is important is when public-~~-~~key encryption 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, even when correctly implemented, will occasionally produce ciphertexts that cannot be decrypted. For most applications, it is important that such decryption failures be rare or absent. While applications can always obtain an acceptably low decryption failure rate by encrypting the same ciphertext multiple times, this type of solution has its 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 or digital signatures~~.~~ (e.g.,, optimized or implicitly authenticated key exchange, etc.).

Commented [BEB57]: 56A and B do not use this term!

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 efficiency.

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

5. Plans for the Evaluation Process

NIST plans to form an internal selection panel composed of NIST employees for the technical evaluations of the submitted algorithms. This panel will analyze the submitted algorithms, review public comments that are received in response to the posting of the ‘‘complete and proper’’ submissions, and all presentations, discussions and technical papers presented at the PQC ~~S~~standardization ~~C~~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 ~~S~~standardization ~~C~~conference, make (any) final selections and document the technical rationale for any such selections in a final report, similar to what- NIST did in the ~~for the selection of~~ AES and SHA-3 competitions. The following is an overview of the envisioned submission review process.

Commented [STM(58]: This is the first time PQC conference is mentioned. I suggest moving this sentence later, or moving the sentence “a PQC Standardization Conference will be held at the .. “ from the next Section before this.

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 ~~section~~Sections 2 and 3 of this notice. NIST will post all ‘‘complete and proper’’ submissions at http://csrc.nist.gov/groups/ST/post-quantum-crypto/ for public ~~inspection~~review. To help inform the public, a PQC ~~S~~standardization ~~C~~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. If an algorithm is not included in the narrowed pool, then it does not mean the algorithm is removed for consideration for standardization~~,~~ unless expressly stated 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.

Commented [STM(59]: How about merging similar submissions ?

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

Commented [BEB60]: 11:11 AMhis seems to contradict the statment two paragraphs above.

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 explanation/ 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 or not 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 shall 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 proposed 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~~section. After the end of the public review period, NIST intends to hold another PQC ~~S~~standardization ~~C~~conference. (The exact date is to be scheduled.)

Following the third PQC ~~S~~standardization ~~C~~conference, NIST will prepare a summary report, which may select algorithm(s) for possible standardization, and/or may determine that another phase of evaluation is needed. This third evaluation process would be structured similarly ~~structured as~~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; however, 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(s) of evaluation is intended, at a minimum, to be performed as follows:

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

Commented [BEB61]: Is this supposed to be a title, which should bolded or numbered or both?

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, ~~D~~digital ~~S~~signal ~~P~~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 specify some of the algorithms using a ~~H~~hardware ~~D~~description ~~L~~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 intended platform/compiler will be noted on http://csrc.nist.gov/groups/ST/post-quantum-crypto/.

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 c~~C~~onference. Details of the c~~C~~onference will be posted at http://csrc.nist.gov/groups/ST/post-quantum-crypto/.

For conference and resource allocation planning purposes, it would be appreciated if those planning to submit algorithms could notify the individuals listed in the **FOR FURTHER INFORMATION CONTACT** ~~section~~Section as soon as possible.

Commented [SC62]: I know this paragraph was in the SHA-3 CFS, but I've always felt that it
can be removed. When we announce a workshop, we will certainly inform the public what to do, and who to contact. There is no need to mention it right here.

Appreciation

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

Commented [SC63]: I'm not keen on keeping this section either. We can always thank the public in our report, but I won't mind if this section stays.

Dated: xxx