From:	Chen, Lily (Fed)
To:	Moody, Dustin; Perlner, Ray; Jordan, Stephen P; (b) (6) ; Liu, Yi-Kai
Cc:	Peralta, Rene; Bassham, Lawrence E
Subject:	RE: My write-up in the PQC call
Date:	Monday, March 28, 2016 4:04:00 PM
Attachments:	llc-CFP v3.docx

Attached please see my comments. Some of them are questions to be discussed tomorrow.
Lily

From: Moody, Dustin (Fed)
Sent: Monday, March 28, 2016 12:38 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Daniel Smith (b) (6) ; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Subject: RE: My write-up in the PQC call
I've added in a few more comments (mostly questions) also.
Note – our meeting location tomorrow is A-318.
Dustin

From: Perlner, Ray (Fed)
Sent: Monday, March 28, 2016 10:19 AM
To: Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Daniel Smith (b) (6) ; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: RE: My write-up in the PQC call
I've added a few more comments
Good luck everyone,
Ray

From: Jordan, Stephen P (Fed)
Sent: Sunday, March 27, 2016 9:49 PM
To: Daniel Smith (b) (6) ; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Re: My write-up in the PQC call
Dear All,
I've added a few additional comments. The resulting file is attached.
Best regards,
Stephen

From: Daniel Smith (b) (6)
Sent: Saturday, March 26, 2016 1:03 AM
To: Liu, Yi-Kai (Fed)
Cc: Moody, Dustin (Fed); Perlner, Ray (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed)

Subject: Re: My write-up in the PQC call

Hello,

Here is my first attempt at giving some sort of minor contribution. A couple of items I didn't know exactly how to handle. The rest is mostly plagiarized from the SHA-3 call so that we at least have a draft to work with.

Also, I'm using Word 2016. I chose compatibility mode,so I hope that there are no issues with this.

Cheers,

Daniel

On Fri, Mar 25, 2016 at 9:29 AM, Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov> wrote:

> Hi everyone,
> Here is a combined version of the document. (Thanks Dustin for your help with this.)
> Could everyone look at it? Please flag any sections that need additional work, and flag any issues that we need to discuss when we meet next Tuesday.
> Many thanks!
> --Yi-Kai
>
> ---
>
> **From:** Liu, Yi-Kai (Fed)
> **Sent:** Thursday, March 24, 2016 5:55 PM
> **To:** Daniel; Moody, Dustin (Fed); Perlner, Ray (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
>
> **Subject:** Re: My write-up in the PQC call
> Hi Daniel,
> No worries. Hope you feel better!
> --Yi-Kai
>
> ---
>
> **From:** Daniel (b) (6) [redacted]
> **Sent:** Thursday, March 24, 2016 4:38 PM
> **To:** Liu, Yi-Kai (Fed); Moody, Dustin (Fed); Perlner, Ray (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
> **Subject:** Re: My write-up in the PQC call
> Hi,
> I'm going to be a little slow on my part. I became ill yesterday, and I'm not able to eat anything. I have no energy, but I'm hopeful that I will recover soon. I'm trying to work, but I need to sleep every couple of hours. I will try to get you my contribution tomorrow. Sorry for the delay.
> Cheers,
> Daniel
> Sent from my T-Mobile 4G LTE Device
>
> -------- Original message --------
> From: "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>
> Date:03/24/2016 2:10 PM (GMT-05:00)

To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)" <daniel-c.smith@louisville.edu>
Cc:
Subject: Re: My write-up in the PQC call
Hi everyone,
Here is my section of the CFP.
Thanks everyone! Daniel, feel free to send it whenever you're ready.
Later today or tomorrow, I'll try to merge everyone's contributions into one document, and send it around.
--Yi-Kai

From: Moody, Dustin (Fed)
Sent: Wednesday, March 23, 2016 11:49 AM
To: Liu, Yi-Kai (Fed); Perlner, Ray (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: FW: My write-up in the PQC call

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, March 23, 2016 11:32 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: My write-up in the PQC call
My sections. Let me know if you need more.
Larry

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 Quantum-Resistant Cryptographic Algorithms.

SUMMARY: This notice solicits nominations from any interested party for quantum-resistant cryptographic algorithms to be considered for new public key cryptographic standards that will be secure against quantum computation. It addresses the nomination requirements and the minimum acceptability requirements of a ''complete and proper'' candidate algorithm submission. The evaluation criteria that will be used to appraise the candidate algorithms are also described.

Commented [SC1]: For the hash competition, we published an FRN just to discuss the evaluation criteria. When this was settled ten months later, we then issued an FRN to call for candidate nomination. I wonder if you want to do that as well.

DATES: Candidate nomination packages must be received by DATE. Further details are available in Section X.

ADDRESSES: Candidate algorithm 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 XXX@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: 301–975–XXX or via fax at 301–975–8670, e-mail: XXX@nist.gov.

SUPPLEMENTARY INFORMATION: This notice contains the following sections:

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, and they play a crucial role in ensuring the confidentiality and integrity of communications on the Internet and other networks.

Due to this concern, many researchers have begun to investigate post-quantum cryptography (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 look promising, including lattice-based cryptosystems, code-based cryptosystems, multivariate cryptosystems, and hash-based signatures. However, further research is needed in order to gain more confidence in their security (particularly against quantum adversaries), and to improve their efficiency and 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 painless, as there is unlikely to be a simple "drop-in" replacement for our current

Commented [MD(2]: Define: encryption, signatures
Need for PQC
Impact on crypto – symmetric, PK
Candidate cryptosystems
Impact on standards, timeline
Development of q computers
Time needed to deploy new crypto
Migration – e.g., hybrid modes are automatically compliant
Will work with industry and other standards organizations (e.g., stateful hash-based signatures)
New NIST standards for public key encryption and signatures
"Pre-quantum" standards are likely to be deprecated
Desirable features
Drop-in replacement in existing applications, as much as possible
Secure against classical and quantum computers
"Standardization process"
Not competition
Comparing apples and oranges
Less understanding of q cryptanalysis

Commented [MD(3]: Mention others? Some people won't be happy with being left off the list…

Commented [CL(4]: Option 1 is not mention any specific algorithms in this section. Option 2 is changing the leading sentence to avoid the term "promising". We can say that "In the recent years, several categories of cryptosystems have been extensively considered, including … …"

public key cryptographic algorithms. In addition, this transition needs to take place well before any large-scale quantum computers are built, so that any information which 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, other efforts to standardize stateful hash-based signatures).

Most importantly, NIST will begin a process to develop new post-quantum standards for 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 TLS, IPSec (IKE), and digital certificates.

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

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 our 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.

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

2. Requirements for Candidate Algorithm Submission Packages

Commented [CL(5]: Yes. We shall include standardization and adoption.

Commented [MD(6]: Not the only reason. For example, getting standards and protocols for the new algorithms will take time. Do we want to mention this also?

Commented [MD(7]: Is beginning?

Commented [MD(8]: Mention key establishment?

Commented [MD(9]: We probably should mention we need them to replace the standards that will be broken, and name those standards (FIPS 186 and SP 800-56 A/B)

Commented [S10]: I would remove the word "our". We really mean humanity's understanding not NIST's understanding.

Candidate algorithm nomination packages must be received 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. Requests for the withdrawal of submission packages will only be honored until the submission deadline.

Due to the specific requirements of the submission package such as Intellectual Property Statements / Agreements / Disclosures as specified in section 2D, 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:// www.nist.gov/ for inspection. To be considered as a ''complete'' submission, packages must contain the following (as described in detail below):

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

Each of these items is discussed in detail below.

2.A Cover Sheet

A cover sheet shall contain the following information:

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

2.B Algorithm Specifications and Supporting Documentation

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 made. It should also include

Commented [S11]: What does "owner" of an algorithm mean? Is this referring to patents? I think this needs to be clarified.

Commented [CL(12]: "Name of the owner, if IP applies, of the algorithm"?

Commented [MD(13]: Compare to SHA-3 FRN. Their 2.B.1 is much longer and describes more what is wanted (not just bullet points)

A few topics to address:
Can call approved primitives (and only approved primitives), should implement padding, etc., in order to achieve security
Want weakened versions for cryptanalysis
Replacing Diffie-Hellman key exchange with key transport

1) a survey of known work on the cryptosystem; 2) any applicable security analysis; 3) a precise security claim against quantum computation; and 4) a performance analysis.

In addition, the submission should include a tunable security parameter which allows the selection of a range of possible security/performance tradeoffs as well as the construction of weakened versions of the submitted algorithm for analysis. If such a parameter is included, the submission document must specify a recommended value with justification. A tunable parameter 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 value than originally specified by the submitter.

A complete submission will include any necessary padding and calls to approved primitives in order to achieve security. If the algorithm cannot be used directly in current protocols as specified in FIPS or NIST Special Publications, the point(s) of failure must be clearly indicated (and a potential compatibility construct offered?).

How to mention replacing Diffie-Hellman key exchange with key transport?

2.B.2 In addition, each submission package is required to include Known Answer Test (KAT) values, which can be used to determine the correctness of an implementation of the candidate algorithm. 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. 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 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. Key size.

Followed by a set of tuples where all values within the tuple shall be clearly labeled (*e.g.*, Plaintext, Key, Ciphertext, etc.).

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

Commented [MD(14]: Do all PQC algorithms have such a parameter?

We tell them to include it, but then a sentence later say "if you include it".

Commented [CL(15]: How about "In addition, the submission should specify selected parameter sets which allow selection of a range of possible security/performance tradeoffs as well as the construction of weakened versions of the submitted algorithm for analysis. If such a selection is included, the submission document must specify a recommended set or sets with justification. 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." (Here I tried to avoid the term "tunable security parameter" and use a more general term "parameter set".

Commented [CL(16]: "padding mechanisms and usage of approved primitives"?

Commented [CL(17]: "If the algorithm cannot be used directly in current protocols as the algorithms specified in FIPS and SPs being used, the point(s) of failure must be clearly indicated." In the original sentence, it is not clear about "protocols specified in FIPS and SPs". We claime that we never standardize protocols but schemes. Every key agreement in 56A is a scheme, not a protocol. Or we completelt change the sentence as "If the algorithm cannot be used as a drop-in replacement for the algorithms and schemes specified in FIPS and SPs, the failure point …"

Commented [CL(18]: This has addressed in v of Section 4.

Commented [BLE(19]: I deleted the Monte Carlo Test (MCT) stuff. We don't tend to have MCTs on asymmetric algorithms now. KATs are good enough (and useful) to help you determine if your implementation is at least mostly correct. At this stage that's all we need. We can discuss MCTs when we get to a validation phase.

Commented [BLE(20]: "candidate" or "submitted"

Commented [BLE(21]: Or security strength?

Commented [CL(22]: How about "parameters"?

Commented [BLE(23]: PublicKey, PrivateKey?

Commented [BLE(24]: I could generate a sample file and we could link to it.

i. If the candidate algorithm calculates intermediate values (e.g., internal rounds) for a computation (e.g., the encryption of a single block), then the submitter shall include known answers for those intermediate values for the computation 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*.

ii. If tables are used in the 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.

2.B.3 A statement of the expected strength (i.e., work factor) of the algorithm shall be included, along with any supporting rationale This statement shall include a description of which of the algorithm and parameter settings, specified by the submitter, the submitter is confident meet or exceed each of the security targets specified in section 4.A.iv, for at least one of the security models specified in section 4.A.ii and section 4.A.iii. If the submitter believes these settings exceed the relevant security target, the submitter shall give an estimate of how much the settings exceed the security target. Additionally the statement shall discuss the additional attack scenarios specified in section 4.A.v.~~,~~

2.B.4 An analysis of the algorithm with respect to known attacks (e.g.,~~ differential cryptanalysis~~) and their results shall be included.

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, with justification of why these were not chosen to make some attack easier.

The submitter shall provide a list of known references to any published materials describing or analyzing the security of the submitted algorithm. 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.

A statement that lists and describes the advantages and limitations of the algorithm shall be included. Such advantages and limitations may address the ability to:
Implement the algorithm 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 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).

If the submitter believes that the algorithm has certain features that are deemed advantageous, then these should be listed and described, along with supporting rationale.

Commented [PR(25]: This is a very symmetric-crypto oriented example.

Should think more in terms of internal functions (e.g. message padding in an encryption function, creating an initial commitment/ processing a final challenge hash in a fiat-shamir signature construction etc.) Prime generation in RSA etc.

Commented [PR(26]: Section 4 is now organized a bit differently.

Previously the sections cited gave a variety of specific applications and attacks we were interested in. (This was largely because hash functions are usually modeled as random oracles, despite this not being a standard model functionality. Thus there is no succinct way to describe everything we want from a hash function that isn't provably impossible to satisfy.) Standard public-key security models don't have this problem.

Here's how section 4A is organized now:

Section 4A. ii and iii give security models (implicitly defining, rather than enumerating, what constitutes an attack) We'd expect submitted algorithms to satisfy one of these definitions, but not both.

4A. iv gives our security targets and our thoughts about how to measure the complexity of a quantum attack.

4A.v talks about attacks not covered by the security model, but which are still of some concern

Commented [CL(27]: We may not need "known", just "a list of references" will be fine. Suggest to remove

Some examples of these features might include, for example: ~~Mathematically (rather than empirically) designed tables, statistical basis for inter-round mixing, etc.~~

Commented [d28]: (I'm basing this comment on the type of example marked for deletion here.) Do we want to go into this kind of analysis? Maybe we do. We will hear a lot of arguing on these points in post-quantum, though. There will be complaining about the huge key sizes of the oldest and most trustworthy code-based schemes, the disconnect between lattice reduction complexity in theory and practice, etc. These are (sometimes) valid points, but I wonder if it's useful to suggest contentious topics when asking for advantageous features. Maybe we should just get rit of the entire sentence… or paragraph. Besides, isn't this what the previous paragraph is about anyway?

2.C Optical Media

All electronic data shall be provided on a single CD-ROM or DVD labeled with the submitter's name, and the algorithm name.

2.C.1 Implementations

Commented [BLE(29]: We can discuss if we want an "Additional Implementations" for additional code optimized for other platforms.

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 candidate algorithm may be implemented. Since this implementation is intended for reference purposes, clarity in programming is more important than efficiency. 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 candidate algorithm. This includes support for all core features of the algorithm, e.g., key generation, public key validation, digital signature generation, digital signature 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 <web_page>. 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.

Commented [BLE(30]: Insert appropriate web page for the project.

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

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

2.C.2 Known Answer Tests

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

The required format for the test vectors will be specified by NIST at *http://www.nist.gov/XXXX*.

The 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 PDF. 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.

This electronic version of the supporting documentation shall be provided in a directory \Supporting_Documentation

2.C.4 General Requirements for Optical Media

For the portions of the submissions 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.

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) 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.

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 algorithm, reference implementation, and optimized implementations that I have submitted, known as ____ (print name of algorithm)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if appropriate)_____ .

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

I do hereby understand that my submitted algorithm may not be selected forstandardization 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 algorithm. 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 algorithm's specifications (e.g., to protect against a newly discovered vulnerability).

I understand that NIST will announce any selected algorithm(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 algorithm, 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 algorithm, 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 algorithm from consideration for standardization. . If my algorithm (or the derived algorithm) 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). Additionally, should the U.S. Government not select my algorithm for standardization at the time NIST ends the evaluation process , all rights revert to the submitter (and other owner[s] as appropriate).

Commented [MD(31]: Better name?

Commented [d32]: Isn't this a complicated point since we have an open-ended process in which we may want to select multiple things to standardize?

Signed:
Title:
Dated:
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 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 algorithm known as _____(print name of algorithm) _____ is selected for standardization, an irrevocable nonexclusive royalty-free license to practice the referenced algorithm, 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 algorithm, 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.

Classified and/or proprietary submissions will not be accepted.

2.F Technical Contacts and Additional Information

For technical inquiries, send e-mail to XXX@nist.gov, or contact XXX, National Institute of Standards and Technology, 100 Bureau Drive—Stop XXX, Gaithersburg, MD 20899–XXX; telephone: 301–975–XXX or via fax at 301–975–8670, e-mail: XXX

3. Minimum Acceptability Requirements

Those packages that are deemed to be ''complete'' will be evaluated for the inclusion of a ''proper'' post-quantum public key algorithm. To be considered as a ''proper'' post-quantum public key algorithm submission (and continue further in the standardization process), candidate algorithms shall meet the following minimum acceptability requirements:

i. The algorithms shall be publicly disclosed and available worldwide without royalties or any intellectual property restrictions.
ii. The algorithms shall be implementable in a wide range of hardware and software platforms.
iii. The algorithms shall provide at least one of: public key encryption, digital signatures, or key exchange.
iv. Theoretical and empirical evidence shall be provided to justify security claims of meeting the target security levels.

A post-quantum public key algorithm submission package that is complete (as defined above) and whose algorithm 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 XXX for public review.

4. Evaluation Criteria

NIST will form an internal selection panel composed of NIST employees to analyze the candidate algorithms; the evaluation process will be discussed in section 6. All of NIST's analysis results will be made publicly available.

Although NIST will be performing its own analyses of the candidate 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.

This is not a competition with NIST as judge. We see our role as managing a process of achieving community consensus in a transparent and timely manner. We do not

expect to “pick a winner”. Ideally, several algorithms will emerge as “good choices”. We may pick more than one of these for standardization.

Commented [PR33]: May want to change this wording. I feel like we may not want to say this isn’t a competition any more than we want to say it is.

Commented [CL(34]: We can specifically say what we expect.

4.A Security

The security provided by an algorithm is the most important factor in the evaluation. Algorithms will be judged on the following factors:

i. 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 internet protocols, such as TLS, SSH, IPSec, and DNSsec. Candidate algorithms 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 candidate algorithms to standardize.

ii. Security Model for Encryption

One particularly important application of public key cryptography is general-purpose encryption. NIST intends to standardize at least one algorithm which enables semantically secure encryption with respect to adaptive chosen ciphertext attack (This property is generally denoted IND-CCA2 security in academic literature.)

Commented [CL(35]: This term may be confusing. Why “general-purpose encryption”? It will be used to transport or establish keys, which is not as general as encrypting data.

Candidate algorithms 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. For the purpose of estimating security levels, 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.

iii. Security Model for Digital Signatures

One particularly important application of public key cryptography is digital signtures. NIST intends to standardize at least one algorithm which enables existentially unforgeable digital signature with respect to adaptive chosen message attack (This property is generally denoted EUF-CMA security in academic literature.)

Candidate algorithms for digital signature will be evaluated based on how well they appear to provide this property, when used as specified by the submitter. For the purpose of estimating security levels, it may be assumed that the attacker has access to signatures for no more than 2^{64} chosen messages, however attacks involving more signatures may also be considered.

Commented [CL(36]: I think this shall be “chosen messages (for signatures)”.

iv. Measuring Bits of Security against Quantum Cryptanalysis

Submitters are asked to provide parameter sets that meet or exceed each of five security targets:

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 targets, the intent is that parameter sets meeting security targets 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 targets 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.

NIST recognizes that there is some uncertainty regarding the best way to measure the complexity of cryptanalytic attacks, especially those involving quantum computers. The NIST team's initial thoughts are as follows:

The defining case for *s* bits of quantum security is taken to be a key search for a 2*s* bit key. The most cost effective way to do this using a quantum computer is probably to divide the key space into *p* segments, each of which would be searched for the correct key using a parallel instance of Grover's algorithm. This would then suggest that *s* bits of quantum security should be defined as follows:

An algorithm has s bits of quantum security if an attacker with quantum computational resources proportional to p requires time proportional to $2^s/(p^{1/2})$ *to violate the algorithm's security model.*

Constants of proportionality would be set so that AES 128 has 64 bits of quantum security. Ideally, the submitted parameter sets should meet the above definition for any value of *p*, 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.

It should also be noted that the above definition often has the effect of assigning less quantum security than classical security to an algorithm, even in the absence of a practical quantum speedup. For example, a quantum computer would offer little, if any, advantage to an attacker attempting to find collisions in a 256 bit hash function. Nonetheless, the above definition would still assign something like 80 rather than 128 bits of quantum security, simply based on the fact that classical parallel collision

search uses parallel computation more efficiently than would be expected for a quantum algorithm of the same serial complexity.

Finally, there is an additional area of ambiguity in assessing quantum security. Mathematically, classical attacks may be treated as a special case of quantum attacks. However, it is very likely that classical operations will remain significantly cheaper to implement than explicitly quantum operations, due to the need for error correction and special purpose hardware. The question then arises as to how much this discrepancy should be taken into account. NIST acknowledges that this is a difficult question, however, as the quantum security targets are meant as a safeguard against the "optimistic" scenario, where quantum computing is relatively cheap and ubiquitous, submitters should err towards a small discrepancy, when estimating quantum security.

v. Additional Attack Scenarios

While the previously listed security definitions cover many of the attack scenarios which will be used in the evaluation of candidate algorithms, there are several other properties which 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 algorithms with a slow key generation procedure, 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 attack. Attacks which 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.

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. Algorithms should ideally not fail catastrophically due to isolated coding errors, random number generator malfunctions, nonce reuse etc.

vi. Evaluations Relating to Attack Resistance

Algorithms will be evaluated against attacks or observations that may threaten existing or proposed applications, or demonstrate some fundamental flaw in the design.

Claimed attacks will be evaluated for their practicality and for their impact on applications. Attacks that violate the security of an existing FIPS or NIST Special Publication's use of public key cryptography will be given more weight than attacks that violate the security of other applications; and attacks on rare or obscure applications may be given relatively little weight.

Algorithms will be evaluated not only for their resistance against previously known attacks, but also for their resistance against attacks discovered during the evaluation process, and for their likelihood of resistance against future attacks.

vii. Other Consideration Factors

In addition to the evaluation factors mentioned above, the quality of the security arguments/proofs, the clarity of the documentation of the algorithm, the quality of the analysis on the algorithm performed by the submitters, the continuity of the algorithm's design with previously analyzed constructions, the simplicity of the algorithm, and the confidence of NIST and the cryptographic community in the algorithm's long-term security may all be considered.

Commented [PR37]: For now I just added this one sentence to section vii (adapted from SHA3 FRN 4A section v). May consider expanding it further.

4.B Cost

As described in section 5.A, submitters may periodically submit revised optimized implementations for use in subsequent stages of the evaluation process. In the following discussion, it should be noted that all technical evaluations are performed either on the optimized implementations that are received initially, or on the revised implementations.

Commented [PR38]: Check whether this is true. Surely we will consider other implementations (e.g. in hardware.) I got this from the SHA3 FRN. I think what we're trying to say is that if we have a choice betweenmeasuring the reference and optimized implementation, we care about the performance of the optimized implementation.

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 require radically different performance tradeoffs, NIST may need to standardize more than one algorithm to meet these diverse needs.

i. Public Key, Ciphertext, and Signature Size

Algorithms will be evaluated based on the sizes of public keys, ciphertexts, and signatures that they produce. All of these may be important 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.

ii. Computational Efficiency of Public and Private Key Operations

Algorithms 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.)

iii. Computational Efficiency of Key Generation

Algorithms will also be evaluated based on the computational efficiency of their key generation operations, where applicable. As noted in section 4.c (v), the most common scenario where key generation time is important is when a public key encryption algorithm is used to provide perfect forward secrecy. Nonetheless, it is possible that key generation times may also be important for digital signature algorithms in some applications.

iv. 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.

Commented [PR39]: Need to decide what constitutes an acceptably low decryption failure rate? 2^-64?, 2^-80? 2^-128?

4.C Algorithm and Implementation Characteristics

i. Flexibility

Assuming good overall security and performance, candidate algorithms with greater flexibility will meet the needs of more users than less flexible algorithms, and therefore, are preferable.

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

a. The algorithm 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, identity based encryption, group signatures etc.)

b. It is straightforward to customize the algorithm’s parameters to meet a range of security targets and performance goals.

Commented [CL(40]: Please notice that IBE and group signatures are not currently covered by NIST standards. For flexibity, I do not know whether we consider being able to extend to those schemes as an advantage. Let’s discuss at the meeting.

c. The algorithm can be implemented securely and efficiently on a wide variety of platforms, including constrained environments, such as smart cards.
d. Implementations of the algorithm can be parallelized to achieve higher performance efficiency.

ii. Simplicity

A candidate algorithm will be judged according to its relative design simplicity.

5. Plans for the Candidate Evaluation Process

NIST plans to form an internal selection panel composed of NIST employees for the technical evaluations of the candidate 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 Candidate Conferences, as well as other pertinent papers and presentations made at other cryptographic research conferences and workshops. NIST will issue a report after each ~~SHA-3~~ Candidate Conference, make (any) final selections and document the technical rationale for any such selections in a final report, similar to what NIST did for the selection of AES and SHA-3. The following is an overview of the envisioned candidate review process.

Commented [MD(41]: Do we have a name we can use?

5.A Overview

Following the close of the call for candidate algorithm 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://XXX for public inspection. To help inform the public, a Candidate 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 candidate algorithms. During this initial review period, NIST intends to evaluate the candidate algorithms as outlined in Section 5.B. NIST will review the public evaluations of the candidate algorithms' cryptographic strength and weaknesses, and will use these to narrow the candidate pool for more careful study and analysis.

Commented [MD(42]: Do we want to say here that if an algorithm isn't one of the ones focused on that it isn't out?

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 [MD(43]: Is this what we want? Or will we allow some?

For informational and planning purposes, near the end of the initial public evaluation process, NIST intends to hold another Candidate Conference. Its purpose will be to

publicly discuss the candidate algorithms, and to provide NIST with information for narrowing the field of algorithms to be focused on.

NIST plans to narrow the field of ~~candidates to approximately five~~ candidate 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.

Before the start of a second evaluation period, the submitters of candidate algorithms will have the option of providing updated optimized implementations for use during the next phase of 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 candidates. 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 the candidate algorithms as outlined in the next section. After the end of the public review period, NIST intends to hold another Candidate Conference. (The exact date is to be scheduled.)

Following the third Candidate 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 similarly structured as 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.

It should be noted that this schedule for the candidate 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 the evaluation process will be from three to five years. However, due to developments in the field, this could change.

Commented [MD(44]: I'm not sure we want to pick a number.

Commented [MD(45]: Will not be accepted into the narrowed down candidate pool, but still can be submitted. Right?

Commented [PR(46]: This suggests that we're done after 3 to 5 years. We had previously said we'd have something selected for standardization by then, but we wouldn't necessarily be done. i.e we might evaluate the not-yet selected candidates and decide to standardize one of them later.

Is the evaluation process only 3 to 5 years or is it ongoing?

Commented [CL(47]: How about "NIST estimates that after three to five years of evaluation, some algorithms will be selected for standardization"?

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.

Commented [MD(48]: Anything else we should include? Signature size? Ciphertext size?

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

Platform and Compilers

The above tests will initially be performed by NIST on the

NIST Reference Platform: 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 candidate algorithms when implemented in hardware. During the second evaluation period, NIST may specify some of the algorithms using a Hardware Description Language, to compare the estimated hardware efficiency of the candidate 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://XXX*

5.C Initial Planning for the First Candidate Conference

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

6. Miscellaneous

This section is intended to address some of the questions/comments raised in the review of the draft evaluation criteria.

- When evaluating algorithms, NIST will make every effort to obtain public input and will encourage the review of the candidate 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.
- NIST intends to develop a validation program for algorithm conformance testing, with the goal of having testing available by the time the final standards are published.
- NIST does NOT have a fixed timetable for the completion of evaluation of submissions~~the hash function competition~~. NIST reserves the right to extend the length of the technical review period ~~for each round~~.

- ~~If necessary, NIST may also insert additional rounds of such technical evaluations.~~
- ~~NIST does not intend to select a wholly distinct algorithm for each of the minimally required message digest sizes. It is strongly recommended that no submission be so constructed.~~
- NIST will not target a specific application or platform for implementing the candidate algorithms, as the evaluation of candidate algorithms takes place. One factor that will be taken into consideration for each candidate algorithm is its flexibility—the ability to implement the algorithm securely and efficiently on a wide variety of platforms and applications (see Section 4.C).
- Quantum security models…
- Submissions of hybrid modes are not in the purview of the post-quantum standardization process and will be rejected without consideration. Hybrid modes can be approved for use under existing NIST guidelines.
- The use of complicated primitives such as block ciphers within a submitted algorithm should be restricted to NIST approved primitives. New such constructions requiring independent analysis will not be considered.
- If circumstances arise (such as an advance in security assurance or the discovery of a security flaw) that could not be satisfactorily addressed by modifying NIST's selections for public key encryption, digital signatures or key transport, NIST would likely consider other submitted algorithms. If a significant period of time has elapsed since the selection, NIST would likely examine other algorithms that may have been developed in the intervening period.

Commented [MD(49]: Add details – like co-location with PQCrypto?

Commented [CL(50]: Are we going to address the comments here?

Commented [d51]: What exactly do we want to say here?

Commented [d52]: I don't quite like what I've plagiarized from the previous document here. It is a true statement and should be clear to everyone, but I would like to say something about how we will continue to consider submissions even while standardizing other choices. The problem is that that starts to get complicated legally. What is our stance on this since we want to be able to have access to possibly multiple choices but the developers may want their intellectual rights back if their scheme isn't the first to be standardized?

- ~~Since SHA-3 is intended to augment the existing NIST-approved hash algorithm toolkit, which includes the SHA-2 family of hash functions, NIST does not intend to select an additional "backup" hash algorithm for SHA-3. If circumstances arise (*e.g.*, a discovery of a significant security flaw) that could not be satisfactorily addressed by modifying the selected SHA-3 algorithm, NIST would likely consider the other finalist algorithms. If a significant period of time has elapsed since the hash algorithm selection, NIST would likely examine other algorithms that may have been developed in the intervening period.~~
- Exportability decisions regarding submissions and, eventually, products implementing any selected algorithm(s) will be made by the appropriate U.S. Government regulatory authorities. NIST is a non-regulatory agency of the U.S. Department of Commerce.
- If no appropriate algorithms are submitted in response to this call, NIST expressly reserves the right to cease this process and examine other possible courses of action.
- Submitters are strongly encouraged to submit only one algorithm each (presumably the one in which the submitter has the greatest confidence). The submission of similar, yet distinct, algorithms by the same submitter may delay the public evaluation process and may well raise public questions as to the submitter's level of confidence in his/ her candidates.
- Multiple submitters of sufficiently similar algorithms may be asked to merge submissions. The submission of similar algorithms with distinct parameters and/or analyses may delay the public evaluation process and may well raise public questions as to the submitters' levels of confidence in the submissions.
- For conference and resource allocation planning purposes, it would be appreciated if those planning to submit candidates could notify the individuals listed in the FOR FURTHER INFORMATION CONTACT section as soon as possible.

Commented [MD(53]: Maybe add something similar here…How we could add other algorithms later.

Commented [MD(54]: Is this what we want? I don't think so.

Commented [d55R54]: I think that this bullet point should be deleted entirely. This bullet point should be replaced with the mergers point that we discussed. I think that the same logic applies. If many submitters are suggesting the same algorithm essentially with slightly different parameters, do the authors understand the security/performance?

Appreciation

NIST extends its appreciation to all submitters and those providing public comments during the ~~SHA-3~~ development process.

Dated: xxx