Summary of Draft Call for Proposals Comments and Changes

NIST would like to thank those who submitted comments regarding the draft submission requirements and evaluation criteria for its post-quantum cryptography standardization process. The submitted comments have been compiled and posted at www.nist.gov/pqcrypto. In this document, we summarize the comments received and describe the changes NIST made as a result.

Many of the comments NIST received focused on a lack of clarity in the language in the draft proposal. For instance, a number of commenters had concerns with our use of terminology. This included the usage of “perfect forward secrecy” which did not include any explanation of its meaning, as well as being consistent with how the terms“quantum-resistant,” “quantum-safe,” and “post-quantum” were used. Several commenters requested clarification of potentially confusing language. For instance, there were requests for clarification on the language pertaining to submissions that provide implementations of more than one of the desired cryptographic functionalities. These issues were all dealt with in a very straightforward manner, and fixed in the final call for proposals as necessary.

In turning now to the issues that involved more substantive concerns, we begin with those we could not or otherwise did not accommodate in our revised final call for proposals.

There were a significant number of suggestions relating to the implementation of algorithms. For instance, a number of commenters requested that we recommend or require constant-time implementations of algorithms. While we chose not to require constant-time implementations, we did modify the document to address the constant-time issue and make it clear that we view such implementations as preferable.

Several commenters suggested requiring implementations on a wider range of computing devices than the Intel x64 processor. In particular, they would like to see implementations on more constrained mobile and IoT (Internet of Things) devices. Again, while we chose not to make it a requirement, we did explicitly give them an option of submitting additional implementations on other platforms, and noted that it may be useful.

Some commenters strongly requested that royalty-free licensing be a requirement in our proposals. After consultation with legal experts, we left the language as is. However, we more strongly indicated our preference for algorithms which are royalty-free, and NIST expects that there will be at least one type of algorithm of each functionality selected for standardization which is available without royalties.

A number of commenters took issue with NIST’s initial request for public-key encryption and key-agreement/key exchange, in a number of different manners. One of the criticisms was that our request for public-key encryption and key-exchange schemes was in some sense both too vague and too narrowly defined. Some of the commenters preferred the use of the KEM (key encapsulation mechanism) terminology and definition to the use of the public-key encryption and key exchange. In the interest of broader applicability, we left in public-key encryption, but we replaced the somewhat imprecise request for key exchange with the more explicitly and concretely defined KEM framework.

Commenters also pointed out that for a one-time use KEM (or a one-time use public-key encryption scheme), semantical security with respect to adaptive chosen ciphertext attack (known as IND-CCA2 security) is unnecessary, even while agreeing that general public-key encryption or long-term KEM schemes should indeed satisfy IND-CCA2 security. In particular, it was noted that an already-existing candidate post-quantum KEM scheme does not satisfy IND-CCA2 security, yet this does not cause a security problem for one-time use cases. NIST agrees regarding the lack of a need for IND-CCA2 security for fully ephemeral encryption/key-establishment schemes and made additional specifications relating to their security model which only requires IND-CPA security.

The greatest number of comments dealt with quantum security and the target security strengths. Many comments expressed confusion about the definition of security strength in terms of the cost of breaking various symmetric cryptographic primitives. Others questioned the rationale of NIST’s approach on how to define quantum security.

A handful of commenters wondered whether or not separate parameters were required for all 5 levels of security in a given submission. Still others questioned the specific amounts of quantum or classical security required, as well as our choices for pairing quantum and classical levels of security. For instance, some noted that it is generally difficult, if not impossible, to tune classical and quantum parameters separately.

After much discussion, NIST continues to ask for five security strength categories. However, we did make significant changes to address the concerns raised by the comments. We clarified that submitters are not required to provide different parameters for all five security strengths. Also, in the draft proposal, we had specified each target security level with the number of bits of both classical and quantum security required, and then attempted to relate these to breaking the standard symmetric cryptographic primitives AES and SHA-2/3. In our final call for proposals, we specify each of the five security strength categories entirely in terms of the computational resources required to break each standardized cryptographic primitive.

We also significantly revised the section pertaining to security strength in order to address many of the concerns raised by commenters. To address misconceptions as to our rationale, we explicitly describe our security goals. We also try to address some of the confusion to the levels of security requested by providing suggestions for conversion factors between quantum and classical gates and circuit depth and the amount of computational resources required to break each of the standardized cryptographic primitives.

We received comments regarding decryption failures, including a request for a threshold of the maximum probability of decryption failure that would be tolerated. While we declined to specify any concrete threshold, we did require that any non-zero failure rated be explicitly given in the submission, along with the security impact of such failures. As such failures are usually very tunable via shifts in parameter, we felt it made sense to defer a decision on the maximum acceptable decryption failure rate to later in the process.

Finally, we had a number of commenters suggest that we provide greater emphasis on any submitted scheme's suitability for use in currently existing protocols and applications. We agreed with the suggestions and explicitly added ease of incorporation into current protocols and applications as a positive flexibility factor.

We note that this summary does not cover every topic raised by the comments received by NIST, but is intended to address the more substantive issues brought forward. Some further explanation can be found at the Frequently Asked Questions (FAQ) section of our website: www.nist.gov/pqcrypto.