16 September 2016

National Institute of Standards and Technology
Computer Security Division

Subject: Comments on *Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*

Microsoft Corporation appreciates the opportunity to submit comments on the subject draft. We believe that this standardization process is both timely and critically important. NIST's past standardization activities for AES and SHA-3 were outstanding examples of evaluations of candidate cryptographic algorithms, and the algorithms selected through these processes are now being deployed throughout industry worldwide. We look forward to a similar outcome from this process, and an open and transparent process with clear technical guidelines and evaluation criteria will help ensure that the results of this process are trusted and credible.

Executive summary and high-level recommendations

We have suggestions that we believe will improve the proposed standardization process and the outcome. Our comments focus on the following areas:

- Intellectual Property Rights
- Performance Measurement
- Evaluation Under Real-World Scenarios
- Security Levels
- International Standardization

A. Intellectual Property Rights:

The current draft includes the following statement on Intellectual Property in Section 2.D:

> *NIST has observed that royalty-free availability of cryptosystems and implementations has facilitated adoption of cryptographic standards in the past. As part of its evaluation of a PQC cryptosystem for standardization, NIST will consider the assurances made in the statements by the submitter(s) and any patent owner(s), with a strong preference for submissions as to which there are commitments to license, without compensation, under reasonable terms and conditions that are demonstrably free of unfair discrimination.*

Further, the proposed required Statement by Patent Owner(s) in Section 2.D.2 explicitly allows for a patent holder to select an option of RAND (reasonable and non-discriminatory) licensing with compensation.

This is a change from the SHA-3 competition in that royalty-free licensing is not required by the proposal but is merely a factor to be considered. We have seen in the past how

ambiguity and licensing have hampered the adoption of new cryptographic technologies. It is critical that NIST maintain the same intellectual property rights disclosure and release requirements that were set out for the SHA-3 competition, namely that all submitters be required to release any and all IP claims as a condition of entry, and that each submitter agree to unrestricted, royalty-free use of their work.

Additionally, we note that the proposed approach to Intellectual Property Rights for this competition conflicts with NIST's stated commitment in NISTIR 7977 on this specific issue. See NISTIR 7977, Section 7 ("Policies and Procedures for the Life Cycle Management of Cryptographic Standards and Guidelines), Subsection 4 ("Define a Specific Plan and Process"), bullet point "Hold a Competition" (bottom of page 18 of NISTIR 7977), where NIST writes [emphasis added]:

> If NIST decides to pursue the development of a standard or guideline, it may use an open competition. When a competition is used, interested parties will have an opportunity to participate in the competition by reviewing core requirements and evaluation criteria, publishing research papers, submitting comments, and attending public workshops. Researchers worldwide may contribute candidate designs and papers on the theory, cryptanalysis and performance of the candidates. The winning submitters are recognized, ***but agree to relinquish claim to intellectual property rights for their design so that the winning candidate can be available for royalty-free use***.

This process is clearly a competition as defined in NISTIR 7977, so NIST must adhere to the IPR commitments it made for competitions in that document. To that end, Microsoft strongly suggests that the "reasonable terms and conditions" IPR language be struck from the proposal in favor of the exact language used in the SHA-3 competition, guaranteeing that the selected algorithms be "available on a worldwide, non-exclusive, royalty-free basis."

B. Performance Measurement

i. Constant Time Implementations

Section 2.C.1 ("Implementations") references "optimized implementations" that will be used for performance benchmarking. Real-world applications of cryptographic schemes require constant-time implementations as a minimum to protect against timing and cache-timing attacks.

To ensure that "optimized implementations" reflect what would be deployed, and to enable apples-to-apples comparisons, all "optimized implementations" submitted for this effort should be designed to be constant-time. Second-round updates to submissions may make updates to fix constant-time-related bugs in first-round submissions.

ii. Performance Tooling

The performance evaluation of "optimized implementations" must be done by NIST directly or by an independent and neutral third party not affiliated with any party involved in any submission. The tools used in this evaluation must be open, independent, auditable and neutral, their code must be freely published for inspection, and must not be owned by or affiliated with any party involved in any submission. No submitter can be involved in performance evaluation in any capacity.

iii. Performance Testing Scenarios

The performance evaluation should cover the following platforms at a minimum: a 64-bit processor "server class" and a 32-bit processor "mobile class". In addition, testing should be conducted on 8-bit and 32-bit microcontrollers, and be evaluated on at least one alternative hardware platform (e.g., FPGA).

C. Evaluation Under Real-World Scenarios

i. Hybrid Modes:

In Section 1, NIST writes that "hybrid modes" which combine quantum-resistant cryptographic algorithms with existing (not necessarily quantum-resistant) cryptographic algorithms are out of scope for the competition. We believe this limitation is overly restrictive for two reasons. First, some proposed quantum-resistant schemes may have benefits when combined with certain classical schemes, and NIST's evaluation process should be able to consider such benefits[1]. Second, ease of integration and engineering compatibility with classical cryptography must be a consideration in the evaluation of submitted algorithms as a desirable property. It is most likely that post-quantum cryptographic schemes will be deployed in such hybrid modes first and be used alongside classical cryptography for a significant amount of time. Candidate quantum-resistance schemes must be evaluated in the wider context in which they will be applied, which will include integration with classical cryptography.

ii. Protocol Scenarios

NIST should identify several high-priority protocol scenarios, such as TLS, for evaluating and testing submitted schemes. Ease of integration with the most commonly used security protocols and performance in such scenarios must be an important evaluation criteria.

---

[1] For a practical example of such ancillary benefits see C. Costello, P. Longa and M. Naehrig, *Efficient Algorithms for Supersingular Isogeny Diffie-Hellman,* recently presented at Crypto 2016 and available online at http://eprint.iacr.org/2016/413. In this paper the authors present a post-quantum key agreement scheme based on supersingular isogenies, and in Section 8 they present a strong ECDH+SIDH hybrid ("BigMont") that leverages the underlying field arithmetic of the post-quantum scheme to provide a parallel ECDH key exchange for very little overhead. NIST's current proposed language would prohibit NIST from considering hybrid benefits from such schemes.

In the second round, those candidates selected to continue on should be asked to apply their submissions to selected real-world protocols, such as TLS, to further the evaluation.

D. Security Levels

In Section 4.A.4 ("Target Security Strengths"), NIST identifies five target security strengths for which submitters will be asked to provide parameter sets. We are concerned that the lowest security strengths identified are too low: the requirements should encourage strong and conservative security levels. There are also too many security strengths specified. Reducing the number of parameter sets required of submissions will simplify the evaluation. We suggest that NIST remove target levels (1), (2) and (3) and replace them with a target level of 128 bits classical security / 128 bits quantum security, and that this new level be the minimum target level. Target levels 4) 192 bits classical security / 128 bits quantum security and 5) 256 bits classical security / 128 bits quantum security should be consolidated to one level, and then a third higher level should be added to provide more breathing room in the face of continuing cryptanalytic advances. We suggest that this new higher level be 256 bits classical security / 192 bits quantum security.

Any scheme that has an efficiency or technical obstacle, must clearly justify the limitations that prevent it from achieving the desired security level.

E. International Standardization

In our letter of 25 March 2015 and the accompanying formal comments on the then-draft NISTIR 7977, Microsoft stressed the importance of submitting key NIST standards to standards development organizations (SDOs) with international scope, in particular standards that result from competitions. For this competition we strongly encourage NIST to plan to submit the selected algorithms to one or more international SDOs after the resulting FIPS or SPs are completed. There is an opportunity when establishing new post-quantum cryptography standards to have fewer national variations worldwide.

Conclusion

We believe these modifications will strengthen the proposed process, will ensure the strongest technical outcome from the evaluation, and will provide the best transparency and assurance to the community.

Thank you again for the opportunity to submit these comments. We would be happy to discuss these recommended modifications, or any other aspect of the draft, with you.

Sincerely,

Brian A. LaMacchia, Ph.D.
Director, Security and Cryptography, Technology and Research Group
Microsoft Corporation