From: Chen, Lily (Fed)
To: Moody, Dustin (Fed); (b) (6) Perlner, Ray A. (Fed)
Subject: FAQ
Date: Tuesday, July 5, 2016 4:56:35 PM
Attachments: Frequent Asked Questions-07052016.docx

Hi, Dustin and Ray:

I put the FAQ to a word file, inserted some comments and suggested changes. Please take a look.

Let's think about what other questions shall be included.

Thanks,

Lily

Frequent Asked Questions

Q: The call for proposals briefly mentions hybrid modes that combine quantum-resistant cryptographic algorithms with existing cryptographic algorithms (which may not be quantum-resistant). Can these hybrid modes be FIPS-validated?

A: Assuming one of the components of the hybrid mode in question is a NIST-approved cryptographic primitive, such hybrid modes can be approved for use for key establishment or digital signature. In particular, a hybrid mode signature consists of two signatures. It is valid if only if both signatures are valid. FIPS 140 validation can only validate the signature which is currently NIST approved. Similarly, a hybrid mode key establishment scheme derives keying material from two or more secret values established by different key establishment primitives. Even though only NIST approved key establishment primitive can be validated, depending on the way the secret values are included in the key derivation procedure, FIPS 140 validation test may need to be changed to enable the validation. ~~At present, there are only a few ways to do this that will pass validation, and they aren't necessarily the most natural ways to construct a hybrid mode, but NIST is confident that it can be done and is investigating whether additional support should be added for the validation of hybrid modes.~~ In any case, s~~S~~uch validation, however, is only certifying that the NIST-approved portion is correctly implemented and used, and it says nothing about the security of the quantum-resistant portion of the hybrid mode. NIST therefore continues to believe that hybrid mode may be a way for migration and the long term solution to the threat of quantum computers is to provide standards for postquantum public key cryptography, through the process outlined in our call for proposals.

Q: How does NIST plan to convert time and space complexity of known attacks into a single number for quantum and classical security?

Commented [CL(1]: The answer is not about a plan. How about "What is the rationale to convert …" or "What is NIST understanding to convert …"?

A: NIST's definition of s bits of quantum security is "as hard to break as a block cipher with a 2s bit key, assuming a relatively efficient and scalable quantum computing architecture is available." According to the analysis of Zalka [3] the best generic quantum attack on a 2s-bit block cipher requires a quantum circuit with depth*(squareroot (space)) proportional 2^s. This would suggest that quantum security should be defined as the minimum possible value of log(depth*(squareroot (space))) plus a constant (to put the quantum security of AES 128 at precisely 64 bits of quantum security,) accross all quantum and classical algorithms. This formula should only be taken as a rough guess, though, as there are additional factors to consider: Extremely serial and extremely parallel attacks are likely to be of limited practical relevance, even if the above formula rates them as most efficient. Likewise, even under the assumption that a relatively scalable and efficient quantum computing architecture is available, it is still likely that purely classical algorithms will be easier to implement than the formula suggests, and quantum algorithms that, unlike parallel versions of Grover's algorithms, cannot be divided into small, unentangled, subcircuits, will be harder to implement than the formula suggests. NIST plans to take these practical considerations into account when making its evaluations.

Similarly, NIST's definition of s bits of classical security is "as hard to break as a block cipher with an s bit key, assuming quantum computers are not available." This suggests that classical security should be estimated as the minimum value of log(depth*space) plus a constant, over all classical attack algorithms.

Q: Why are hash functions assigned fewer bits of quantum security than classical security?

A: Bernstein [1] is widely cited as demonstrating that the most efficient quantum algorithm for finding hash collisions is the classical algorithm given by Van Oorschot and Weiner[2]. NIST believes this analysis is correct. Nonetheless, NIST's security goal, that schemes claiming s bits of quantum security be at least as secure against cryptanalysis as a 2s bit block cipher leads to differing definitions for quantum and classical security. In particular, quantum search for a 2s bit key does not parallelize well. It is NIST's judgement that, since cryptanalysis in the real world tends to be most successful when it can take advantage of highly parallel implementations for attacks, finding collisions in a 2s bit hash function must be considered easier than searching for the key of a 2s-bit block cipher, even in a world with ubiquitous quantum computing. NIST therefore assigns fewer than s bits of quantum security against collision to 2s bit hash functions.

Q: What are NIST's plans regarding stateful hash-based signatures?

A: NIST plans to coordinate with other standards organizations, such as the IETF, to develop standards for stateful hash-based signatures. As stateful hash-based signatures do not meet the API requested for signatures, this standardization effort will be a separate process from the one outlined in the call for proposals. It is expected that NIST will only approve this standard for use in a limited range of signature applications, such as code signing, where most implementations will be able to securely deal with the requirement to keep state.

Commented [CL(2]: Is this the only reason that we put hash based signature as a separate process?

References

[1] Daniel J. Bernstein, Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? https://cr.yp.to/hash/collisioncost-20090517.pdf

[2] Paul C. van Oorschot, Michael Wiener, Parallel collision search with cryptanalytic applications, Journal of Cryptology 12 (1999) http://people.scs.carleton.ca/~paulv/papers/JoC97.pd

[3] Christof Zalka, Grover's quantum searching algorithm is optimal, Physical Review A, 60:2746-2751, 1999 http://arxiv.org/abs/quant-ph/9711070