

From: [Moody, Dustin \(Fed\)](#)
To: [Kerman, Sara J. \(Fed\)](#)
Cc: [Chen, Lily \(Fed\)](#)
Subject: FAQs
Date: Monday, July 4, 2016 12:05:35 PM

Sara,

I remembered one more thing - we will want to have a FAQ on our website. Here's the first few questions and answers that we would like there. We might occasionally add to it.

Dustin

FAQ

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. 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. Such 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 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?

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*(squereroot (space)) proportional 2^s . This would suggest that quantum security should be defined as the minimum possible value of $\log(\text{depth}*(\text{squereroot (space)}))$ 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 $\log(\text{depth} \cdot \text{space})$ 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 Wiener[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.

[1] Daniel J. Bernstein, Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? <https://cr.yep.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.pdf>

[3] Christof Zalka, Grover's quantum searching algorithm is optimal,

Physical Review A, 60:2746-2751, 1999 <http://arxiv.org/abs/quant-ph/9711070>

From: Kerman, Sara J. (Fed)

Sent: Wednesday, June 29, 2016 12:49:17 PM

To: Moody, Dustin (Fed)

Cc: Chen, Lily (Fed)

Subject: RE: Documents to soon post on PQC webpage

Dustin,

Have you received the date from legal that the FRN will be posted? They usually provide that to the person who submits FRN through legal. I'm swamped right now with the upcoming commission meeting so I'd just like to have a FRN posting date to try to set up my priorities.

Sara

From: Moody, Dustin (Fed)

Sent: Wednesday, June 29, 2016 12:13 PM

To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>

Subject: Documents to soon post on PQC webpage

Sara,

Our FRN notice will soon be posted, and we want to post several things to our PQC page on the same date. Larry has several technical files, which provide some guidance and examples on how to format some parts of the submissions. We'll need those somewhere. They include the files (API, VariableMsg_2048, KAT, VariableLabel_2048, IntermediateValues_2048). They are referenced by the Call for Proposals main document. I haven't attached the main document, as the lawyers gave me several revisions to make. I hope to have it to you later today or tomorrow. I've also attached text that can be used as an announcement (CFP announcement).

If I don't respond quickly, it's because I'm on annual leave! (But I'm checking in at least daily).

Thanks!

Dustin