From: Perlner, Ray (Fed)
To: Moody, Dustin (Fed); (b) (6) Liu, Yi-Kai (Fed); Chen, Lily (Fed); Alperin-Sheriff, Jacob (Fed)
Subject: RE: FAQ update
Date: Friday, October 21, 2016 2:26:22 PM
Attachments: new FAQ-1 Ray.docx

I broke up the material previously in section 4.A.6 among 4 questions added to the Q&A. We may need some additional work on formatting, but. Please let me know if this approach seems good.
Thanks,
Ray

From: Moody, Dustin (Fed)
Sent: Thursday, October 20, 2016 8:10 AM
To: Daniel Smith (b) (6); Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>
Subject: Re: FAQ update

Daniel added a FAQ on the differences with a competition. Reading NISTIR 7977, we certainly share a lot of commonalities with the process described for competitions. I think it's good that we explain what's different.
I've added some revisions/comments. Let me know what you think.

From: Daniel Smith (b) (6)
Sent: Wednesday, October 19, 2016 10:45:18 AM
To: Moody, Dustin (Fed)
Subject: FAQ update

Hi, Dustin,
Here is a draft of a FAQ on the IP issues. This is a contentious point, and we'll probably want to talk about and revise this.
Cheers,
Daniel

Q: Does the requirement for ANSI C source code preclude the use of assembly language optimizations?

A: The optimized code required as part of the submission package should be ANSI C with no assembly (this includes inline assembly). This code is meant to be portable. If significant optimizations can be made with assembly, then it can be included as an additional implementation and discussed in the performance analysis.

Q: Will NIST consider platforms other than the "NIST PQC Reference Platform" when evaluating submissions?

A: The reference platform was defined in order to provide a common and ubiquitous platform to verify the execution of the code provided in the submissions. NIST will include performance metrics from a variety of platforms in our evaluation, including: 64-bit "desktop/server class", 32-bit "mobile class", microcontrollers (32-, 16-, and where possible, 8-bit), as well as hardware platforms (e.g., FPGA). Submitters are encouraged to provide additional implementations for these platforms if possible.

Q: In Sections 4.A.2 and 4.A.3, NIST's CFP sets the number of decryption (resp. signature) queries, that an attacker against a proposed encryption (resp. signature) scheme can make, to at most 2 to the 64. What is the rationale for not letting the adversary make essentially as many queries as the target security?

A) Our reason for primarily considering attacks involving fewer than 2 to the 64 decryption/signature queries is that the number of queries is controlled by the amount of work the honest party is willing to do, which one would expect to be significantly less than the amount of work an attacker is willing to do. Any attack involving more queries than this looks more like a denial of service attack than an impersonation or key recovery attack. Furthermore, effectively protecting against online attacks requiring more than 2 to the 64 queries using NIST standards would require additional protections which are outside the scope of the present postquantum standardization effort, most notably the development of a block cipher with a block size larger than 128 bits. This may be something NIST pursues in the future, but we do not feel it is necessary for addressing the imminent threat of quantum computers. That said, as noted in the proposed call for algorithms, NIST is open to considering attacks involving more queries, and would certainly prefer algorithms that did not fail catastrophically if the attacker exceeds 2 to the 64 queries.

Q: Is the NIST PQC Standardization Process~~In Section 2.D, the section on Intellectual Property Statement, there is no explicit requirement of royalty-free licensing. Doesn't NISTIR 7977 specify that a NIST competition will require submitters to relinquish intellectual property rights?~~ a competition?

Commented [Office1]: The way you framed the question, it is addressing Microsoft's comment. I think we should make the Q&A more general. I don't think we need to mention IPR in the question, as we don't even mention it in the answer.

A) ~~NISTIR 7977 specifies the rules for NIST competitions. NISTIR 7977 does not specify rules for this process which is NOT a competition.~~ This process shares many features with NIST competitions, and is modelled after the successes we have had with competitions in the past. There are, however, some important requirements that the current research climate demands we require for this process which constitute significant distinctions between this process and a competition.

First, our handling of the applicants does not coincide with a competition as specified in NISTIR 7977. There will not be a single "winner". Our intention is to select a couple of options for more immediate standardization, ~~(in competition lingo, one might call these "winners")~~ as well as to eliminate some submissions as unsuitable. ~~(again, in competition lingo, one might call these "losers")~~ T~~but t~~here will likely be some submissions that we ~~cannot classify as either option~~do not select for standardization, but that we also do not eliminate and which may be ~~an~~ excellent options for a specific application that we're not ready or don't have the contemporaneous resources to standardize. In such a circumstance, we

would communicate with the submitters to allow these to remain under a public license for study and practice and to remain under consideration for future standardization. There is no specification for the handling of such an applicant in a competition.

Second, the state of the science in the competitions of the past, i.e. for the ~~block cipher and hash function~~AES and SHA-3 competitions, was far more developed than for~~the~~ post-quantum cryptograph~~nomy~~. Though differences of opinion are inevitable~~,~~, the selection of the past winners ~~it~~ should not have been to~~n~~o surprising~~surprise for anyone involved which options were selected as winners~~. Rijndael was obviously one of the best choices as the winner for the AES competition. Keccak was a leading performer, had solid theoretical security and offered more functionality and originality than ~~any~~ other competitors, and was therefore~~, hence , also obviously one of~~ the best possible selection~~s~~. The situation in post-quantum cryptography is less clear and opinions of required properties are less unanimous. It will likely be the case that NIST's~~our~~ selection is less universally agreed upon, and as such will likely be less universally judged as a fair selection of the best option(s). We cannot, therefore, promise the universal perception of fairness which is naturally implied by a competition; rather, the best we can hope for is to offer selections that most experts can agree are good options, since there will likely be no consensus of what constitutes a best option.

Commented [Office2]: Do we want to mention that the criteria/timeline could change as well, due to the uncertainties in the field?

Commented [Office3]: Should we address the issue that people will call it a competition anyway? Say we prefer the phrase "competition-like" or invent some new word like quasi-competition or something?