From:	Perlner, Ray (Fed)
To:	Moody, Dustin (Fed); Alperin-Sheriff, Jacob (Fed); Bassham, Lawrence E. (Fed); Chen, Lily (Fed); Daniel Smith-Tone; Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Peralta, Rene C. (Fed); Smith-Tone, Daniel C. (Fed)
Subject:	FAQ entry for CCA/CMA query complexity
Date:	Wednesday, October 5, 2016 2:16:32 PM

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.