From:	Barker, William C. (Assoc)
To:	Chen, Lily (Fed); Souppaya, Murugiah P. (Fed); Moody, Dustin (Fed)
Subject:	Re: Question Regarding Crypto Agility
Date:	Thursday, August 1, 2019 10:29:27 AM

Thanks very much, Lily.

From: Lidong Chen <lily.chen@nist.gov>
Date: Thursday, August 1, 2019 at 10:14 AM
To: William Barker <william.barker@nist.gov>, Murugiah Souppaya <murugiah.souppaya@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: RE: Question Regarding Crypto Agility

Hi, Curt,

Please see the answer to the last FAQ. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs

In general 2^64 quantum computing complexity is not equivalent to 2^64 classical complexity in dollar figures. They are more expensive. When we have a good understanding on how much more expensive, we will provide recommendations.

The experts have confirmed that for AES 256, the real complexity would not be 2^128 quantum complexity. It is much higher. AES256 will be still secure as far as the experts understand for the next 20 years. I will try to find the paper and send to you.

Lily

From: Barker, William C. (Assoc) <william.barker@nist.gov>
Sent: Thursday, August 1, 2019 8:52 AM
To: Souppaya, Murugiah (Fed) <murugiah.souppaya@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Dodson, Donna F. (Fed) <donna.dodson@nist.gov>
Subject: Question Regarding Crypto Agility

Most of the discussion I've followed regarding the impact of quantum computing has focused on Shor's algorithms impact on currently standard public key algorithms. I've not seen very much regarding Grover's algorithm's impact on symmetric key algorithms beyond a need to roughly double the key size in order to achieve the same level of protection. Thinking about AES, I think that implies at least an increased block size, number of rounds and key schedule. We've experienced a degree of inflexibility in protocols and some applications with respect to restricting key sizes to integer powers of two (e.g., insistence on use of AES 192 in some applications). Moving to AES 512 or AES 1024 appears to have its own set of implementation issues. Are we currently looking specifically at the applications and protocol implications of increasing AES key size? Is someone here looking at MAC implications?