From: Moody, Dustin (Fed)
To: Perlner, Ray A. (Fed); Liu, Yi-Kai (Fed)
Subject: Target Security Strength section
Date: Thursday, May 12, 2016 1:46:47 PM

Ray and Yi-Kai,

Stephen modified the last couple of paragraphs of section 4.A.4. His changes appear fine to me. I've included the text of the section below. Let me know if you have any problems with it.

Thanks,

Dustin

4.A.4 Target Security Strengths Submitters are asked to provide parameter sets that meet or exceed each of five target security strengths:

1) 128 bits classical security / 64 bits quantum security
2) 128 bits classical security / 80 bits quantum security
3) 192 bits classical security / 96 bits quantum security
4) 192 bits classical security / 128 bits quantum security
5) 256 bits classical security / 128 bits quantum security

In specifying these security strengths, the intent is that parameter sets meeting security strengths 1, 3, and 5 will remain secure as long as brute-force attacks against AES-128, AES-192, and AES-256, respectively, remain infeasible. Likewise, parameter sets meeting security strengths 2 and 4 should remain secure roughly as long as brute-force collision attacks against SHA-256/ SHA3-256 and SHA-384/SHA3-384, respectively, remain infeasible.

Some care is needed to precisely define the meaning of these security strengths. Intuitively, k bits of classical security means that the best cryptanalytic attack requires 2^k classical computing resources, and k bits of quantum security means that the best cryptanalytic attack requires 2^k quantum computing resources. To make this statement precise, however, one must choose an appropriate unit of computational work. To resolve this ambiguity, NIST proposes to *define* the units of computational work to be such that AES-128 has 128 bits of classical security and 64 bits of quantum security. This is plausible under the assumption that there are no attacks on AES that require significantly less work than a brute-force search.

NIST will also consider other factors that affect the feasibility of an attack, such as how easily the attack can be parallelized, and whether the attack can be implemented using special-purpose hardware (such as hybrid quantum-classical architectures, quantum annealers, graphics processing units, neuromorphic architectures, and others). NIST also recognizes that there is some uncertainty regarding the best way to measure the practical feasibility of cryptanalytic attacks, especially attacks using quantum computers.

Parallelizability of attacks is a major concern for NIST. NIST is concerned with the most practical attack on a cryptosystem, which may not be the one requiring the smallest number of operations. In particular, an attack requiring a larger total number of operations may be more practical than one that requires fewer operations if the former is more amenable to speedup via parallel execution (i.e., reducing its time complexity by performing more computations in parallel).

One of the simplest examples of this phenomenon involves hash functions: A quantum preimage attack on a $2s$-bit hash function, using Grover's algorithm, has roughly the same complexity as a classical search for collisions on the same $2s$-bit hash function (ignoring costs associated with reversibility, fault tolerance, etc.). However, Grover's algorithm parallelizes significantly more poorly than classical collision search. As a result, in a realistic scenario where the attacker performs many operations in parallel, classical search for collisions on a $2s$-bit hash has a significantly lower time complexity than quantum preimage search on the same hash function.

NIST's goal is that schemes with parameters assigned *s* bits of quantum security be strictly harder to break than a block cipher with a 2*s*-bit key. Thus, ideally, the submitted parameter sets should meet or exceed the quantum security of a block cipher with a 2*s*-bit key for any degree of parallelism, but NIST recognizes that extremely serial or extremely parallel attacks (e.g., those that have a time depth or space complexity exceeding 2^{100}) may be of minimal practical importance.

It appears that quantum computations will be significantly more expensive to perform than classical computations using current and near-future technologies, due to the need for quantum error correction and distinctive hardware requirements, such as extreme cooling. Therefore, NIST will consider the extent to which attacks can be made less expensive by doing some or all of the computation on hardware (e.g., classical computing hardware) that may be less expensive to produce or maintain than general purpose quantum computing hardware.

However, the development of quantum computing hardware is difficult to predict. For the purpose of developing post-quantum cryptosystems, it may be prudent to plan for the extreme scenario where quantum computers will be relatively cheap and ubiquitous. NIST will therefore take quantum attacks seriously, even if they require the full power of a general purpose quantum computer.