"Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria"

GOUGET Aline <Aline.Gouget@gemalto.com>

Tue 9/13/2016 3:59 AM

To: pqc-comments <pqc-comments@nist.gov>;

Hello,

I have one comment on the document « Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process ».

In Section 4.A.4, five target security strengths are listed. On security strength 2 and 4, it is explained that the reference is brute-force collision attacks against SHA-256/SHA3-256 and SHA-384/SHA3-384.

However, in the paper « Cost analysis of hash collisions : Will quantum computers make SHARCS obsolete ? » by Daniel J. Bernstein (https://cr.yp.to/hash/collisioncost-20090517.pdf), it is explained that :
« There is a popular myth that the Brassard-Hoyer-Tapp algorithm reduces the cost of b-bit hash collisions from 2^(b/2) to 2^(b/3); this myth rests on a nonsensical notion of cost and is debunked in this paper. »

And later in the same paper :
« The best time claimed by Brassard, Hoyer, and Tapp in [6], and by Grover and Rudolph in [10]|is 2(b/2) /M^(1/2) on a size-M quantum computer. »

Based on this paper, it would mean that:
- For level 2 : 128 bits classical security /80 bits quantum security with the reference to a quantum brute-force collision attack on SHA-256/SHA3-256 would require a quantum computer of size 2^96 to find a collision on SHA-256/SHA3-256.
- For level 4 : 192 bits classical security / 128 bits quantum security with the reference to a quantum brute-force collision attack on SHA-384/SHA3-384 would require a quantum computer of size 2^128 to find a collision on SHA-384/SHA3-384

My comment is that a clarification seems needed on the meaning of the target security strengths 2 and 4, assuming that they are kept in the final version.

Regards

Aline Gouget