Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria

Damien Stehlé <damien.stehle@ens-lyon.fr>

Sun 9/4/2016 3:58 AM

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

Dear Madam/Sir,

I have a few of comments on the document
"Proposed Submission Requirements and Evaluation Criteria for
the Post-Quantum Cryptography Standardization Process".

In Sections 4.A.2 and 4.A.3, you set the number of decryption (resp. signature) queries, that an attacker against a proposed encryption (resp. signature) scheme can make, to at most 2^64.
I find this very low compared to the targets of security mentioned in Section 4.A.4. What is the rationale for not letting the adversary make essentially as many queries as the target security?

I am a bit confused by Section 4.A.4. Clearly, the classical and quantum bit security of a given scheme can differ. But why are the ratios 1/2 and 2/3 put forward as targets? This seems driven by search and collision-search, but these algorithms may not be so relevant for the schemes that will be proposed. We could very well imagine that for some proposed schemes, the ratio will be 1, and for others it will be 1/10. As the focus is on quantum security, it may be tempting to focus on quantum bit-security targets, possibly with an additional requirement of not getting below a certain (and higher) classical bit security.

Best regards,
Damien Stehlé