Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria

Peter Schwabe <peter@cryptojedi.org>

Fri 9/16/2016 8:01 AM

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

Dear NIST post-quantum team,

Thank you very much for running this competition. As you are asking for comments on the draft, here are a few things that you might want to consider:

- In Section 4.A.2 ("Security Model for Encryption/Key-Establishment") you are treating Encryption and key exchange together and are asking for IND-CCA2 security. It may be interesting to distinguish the two cases of public-key encryption (to a long-term key, requiring CCA security) and ephemeral key exchange, which needs only passive security. For example, the "NewHope" key exchange by Alkim, Ducas, Pöppelmann and myself, which is currently used in Google's post-quantum experiment, is explicitly *not* offering CCA security. We could, for the sake of the competition, modify it to achieve this goal, but this would sacrifice security and performance for the ephemeral case, where CCA security is not required.
  On August 26, Jacob Alperin-Sheriff sent us (the NewHope authors) an e-mail suggesting that NIST might be intersted in receiving NewHope (or maybe by next year an improved version) as a submission to the competition, but with the current call I don't see how it would fit in.

- Section 4.A.4 asks for submissions at different security strenghts. What I find interesting is that there is no level offering the same security against classical and quantum attacks. For example, imagine an algorithm that offers N bits of security both against classical and quantum attackers. Personally, I want crypto that offers 128 bits of long-term security, so the only way to fit this algorithm into the proposed security levels is to scale N to 192, although most users would be happy with 128-bits of pre-quantum and post-quantum security.

Best regards,

Peter