From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] Procedures for input regarding parameter sets?
Date: Tuesday, November 15, 2022 10:30:02 AM ET
Attachments: smime.p7m

One of NIST's July announcements was "As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1."

Procedurally, how is this supposed to work? The round-3 Kyber-512 security analysis is two years old and obviously doesn't account for newer attack papers such as the Guo--Johansson paper, the MATZOV paper, and the paper https://cr.yp.to/papers.html#lprrr that I've just posted. Is NIST still seriously considering Kyber-512? Does NIST have a schedule for the Kyber team to issue revised security claims for comment by the community? Or does "NIST will seek input" mean that NIST is already asking the community to comment?

There are reports that NIST is considering another round of tweaks to Kyber, not just throwing away Kyber-512. Are these reports correct? If so, when will tweaks be made available for public security evaluation?

As a separate matter, does "particularly for security category 1" mean that NIST doesn't want input from the community regarding category-5 parameters? Previously, NIST wrote that it "strongly encourages" submissions to include category-5 parameters, and wrote the following:

> A controversial assessment of category 5 runs the risk that the submission will not meet the needs of any users who actually want category 5.

https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF now says "Use Level V parameters for all classification levels", which fits the idea that some users "actually want category 5", but then what's supposed to happen if Kyber-1024 doesn't meet category 5?

---D. J. Bernstein