From: Liu, Yi-Kai (Fed)
To: Cooper, David (Fed); internal-pqc
Subject: Re: Algorithms vs. implementations
Date: Monday, June 15, 2020 6:32:58 PM

I'll leave it to Daniel A. to decide on what is the best wording for this one, since he has more expertise on both lattices and side-channels...

--Yi-Kai

From: David A. Cooper <david.cooper@nist.gov>
Sent: Monday, June 15, 2020 5:40 PM
To: internal-pqc
Subject: Algorithms vs. implementations

In the FAQs<https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs> (old Q3 and old Q4) it is at least strongly implied that we do not expect submission teams to be experts at developing implementations. This should mean that decisions to advance or not advance candidates should be based on the characteristics of the submitted algorithms, not on the quality of the implementations provided by the teams. We certainly used information gleaned about the algorithms from implementations of them, but that is a slightly different thing.

I think we need to avoid language that implies a candidate didn't move on because the implementation provided by the submission team wasn't the best. Here are some examples of language that concern me:

  * LAC: This description twice mentions that non-constant-time implementations. We should not imply that LAC did not advance because the submission team had trouble developing a constant-time implementation. Non-constant-time implementations should only be an issue if we believe there is something about the algorithm that makes it more difficult to develop constant-time implementations. But, if that was the case for LAC, then we need to state that.
During the first round of the NIST standardization process, several authors published attacks on LAC that reduced its security below the required levels. These included chosen-ciphertext attacks that worked by artificially increasing the decryption failure rate, and side-channel attacks that exploited the non-constant-time implementations of the error correction procedures in LAC. LAC was subsequently modified to resist these attacks.

During the second round, a few more minor security issues were discovered, including another issue involving variable-time implementation of error correction procedures. These issues were described in the public “official comments” on LAC in round 1 and round 2 of the NIST standardization process.

NIST is concerned that the cryptanalysis of LAC seems to involve precisely those aspects of LAC’s design, particularly the use of error correction, that distinguish it from most other structured lattice-based schemes.