From:	Apon, Daniel C. (Fed)
To:	Alperin-Sheriff, Jacob (Fed)
Subject:	RE: (Related note) Re: Security concerns about LAC
Date:	Tuesday, December 4, 2018 1:06:00 PM

Yeah, sure – I should be in after lunch on Thursday

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, December 4, 2018 12:10 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: (Related note) Re: Security concerns about LAC

Hey Daniel,

I've actually been wondering somewhat in line with the correlation based keys, whether it's possible to implement a CCA attack even against the schemes (like Round5).

Like an adaptive type attack that based on the fact that certain messages DON'T result in decryption failure, it becomes less likely to submit other messages that result in somewhat correlated ciphertexts.

Talk about this on Thursday?

From: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
Date: Monday, December 3, 2018 at 3:56 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Security concerns about LAC

Hi all,

I wanted to share some (growing) concerns over the security of LAC's proposed CCA scheme for security-level 5.
Dustin mentioned that we will meet another time (at least) before finalizing our report for the next round, so I wanted to bring this up for people to think about before that meeting.

Recall that a key, novel design choice in LAC is to use a modulus q that's the largest prime less than 2^8 = 256. That is, so that each coefficient/integer has a 'snug fit' within a single byte.
The LAC team chooses this same modulus (q = 251) for each of their 3 proposed schemes at security-levels 1, 3, and 5.
Now, this seems to work out fairly well so far at security-levels 1 and 3, but it may be the case that a one-byte modulus is too small to properly support 256-bits of security..
(The LAC-5 proposal, as compared to LAC-1 or LAC-3, increases the noise rate as well as its use of

error-correcting codes during decryption to buoy its security claim at level 5, rather than re-parameterizing the modulus or ring-dimension, as other schemes do when moving to higher security-levels..)

In particular, there has been a lot of attention to the decryption-failure CCA attack against LAC-5, and LAC's particularly heavy use of error-correcting codes:

- You can find the history of pqc-forum comments on LAC here: https://groups.google.com/a/list.nist.gov/forum/#!topic/pqc-forum/ELk3ruitqAA
- Recall that the CCA decryption-failure attack against lattice schemes (RLWE in particular) was first pointed out by Scott Fluhrer here: https://eprint.iacr.org/2016/085.pdf
- Moreover, there have been two recent ePrint papers released (by the Saber team) analyzing the CCA decryption-failure attack further:
    - https://eprint.iacr.org/2018/1089.pdf //we knew about this one before our two comparison meetings
    - https://eprint.iacr.org/2018/1172.pdf //this paper is new online as of today

In terms of the first paper – /2018/1089 – it is pretty clear that LAC-5 has significantly less security than other lattice schemes, as the number of ciphertexts (and decryption queries) increases.
However, the real loss of security appears to kick in once the adversary can generate and see decryptions of more than 2^128 ciphertexts (perhaps significantly more) – whereas our call for proposals places a limit on ciphertexts at 2^64.
(And this is not just an artifact of our call for proposals – getting significantly more than 2^64 ciphertexts, and their decryptions, would seem to be hard on the face of things.)
So, at the time of our comparison meetings, we had dropped this issue.

In terms of the (new) second paper – /2018/1172 – the authors show that the decryption-failure probability in Ring-LWE and Module-LWE schemes has been underestimated.
The "natural" way to calculate decryption-failure probability, in the case of *Plain*-LWE schemes, is to compute the decryption-failure probability per each coordinate,
and then – assuming independence of the failures per coordinate – to derive the overall decryption-failure probability. This remains sensible for *Plain*-LWE schemes.
However, for Ring- and Module-LWE schemes, the ciphertext-coordinates during decryption are NOT independent of one another, as the ambient lattice is now somehow structured.
The resulting analysis shows that LAC's stated failure rate is missing a factor of 2^48.
(This, of course, should plug directly back into decryption-failure attack analysis such as /2018/1089, or Fluhrer's work..)

While this doesn't imply a definite security degradation for LAC-5 yet, it's certainly an unusually-large amount of movement in estimates for a single scheme's security in a short amount of time.
It should give us at least some pause about how much we trust LAC.. Some further thoughts:

“Do we care if LAC moves on to the next round, and then LAC-5 is fully broken?”
I think, yes we care.
It’s not a good look for us to move things through a round where ‘security is the most important factor,’ and then have it broken after the fact.

“Do we care if this only affects LAC at security-level-5, while security-levels 1 and 3 remain OK?”
I think, yes we care.
It appears (to me) that LAC would have to be fundamentally re-designed to shore up its security at level 5. Plus, cryptographic algorithms have a history of needing to be adjusted to higher security levels over time, once standardized (consider RSA key lengths).
An important factor in standardizing crypto algorithms should be whether the algorithm is “easily scalable” in the future.

“Isn’t LAC our last non-eliminated submission from Asia?”
Unfortunately, yes..

--Daniel