From: Lorenz Panny <l.s.panny@tue.nl>
Sent: Thursday, December 28, 2017 11:45 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: HILA5

Dear Markku, dear all,

The HILA5 submission document seems to claim that HILA5 achieves IND-CCA security if the KEM output is used as an AES-GCM key:

> "The design also provides IND-CCA secure KEM-DEM [CS03] public key
> encryption if used in conjunction with an appropriate AEAD [Rog02]
> such as NIST approved AES256-GCM [FIP01, Dwo07]."

However, we recently showed that this is not the case:

https://eprint.iacr.org/2017/1214

Our attack is an active key-reuse attack, extending Fluhrer's attack to the modified reconciliation and extra error correction used in HILA5.

We emphasize that our attack does not break the IND-CPA security of HILA5. If HILA5 were clearly labeled as aiming merely for IND-CPA security then our attack would merely be a cautionary note, showing the importance of not reusing keys.

Could the author please clarify what security definition the
HILA5 submission is aiming for?

Sincerely,
Daniel J. Bernstein,
Leon Groot Bruinderink,
Tanja Lange, and
Lorenz Panny

From: Mike Hamburg <mike@shiftleft.org>
Sent: Tuesday, January 30, 2018 10:19 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: HILA5
Signed By: mike@shiftleft.org

Hello PQCers,

This is a positive comment about HILA5.

The HILA5 supporting documentation claims a failure probability of 2^(-27*5) = 2^-135, because it uses a 5-error-correcting code. However, with a 5-error-correcting code, 6 errors are needed to cause a failure, so this should read 2^(-27*6) = 2^-162. Furthermore, this estimate overcounts errors by a factor of 496^6 / (496 choose 6), and the documentation states that 99% of 5-error cases are corrected. This would reduce the failure probability to around 2^-178.

However, failures in LWE systems are correlated, so that the 6-error probability is much higher than the above prediction. I am still working on failure estimates, but my current guess is 2^-158, which is still lower than stated in the HILA5 spec.

Of course, none of this matters unless HILA5 is modified to employ the Fujisaki-Okamoto transform or similar.

Cheers,
— Mike

From: Leo Ducas <leo.ducas1@gmail.com>
Sent: Wednesday, January 31, 2018 3:03 PM
To: pqc-forum
Subject: [pqc-forum] OFFICIAL COMMENT: HILA5

Hi Mike,

I've been wondering for quite a while how to handle correlations formally and tightly in this scenario. I'm looking forward to your work. Thanks !

--Leo

--