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
Hello PQCers,

This is a positive comment about HILA5.

The HILA5 supporting documentation claims a failure probability of $2^{-(27\times5)} = 2^{-135}$, 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 $2^{-(27\times6)} = 2^{-162}$. Furthermore, this estimate overcounts errors by a factor of $496^6 / \binom{496}{6}$, 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
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
Hi.


Cheers,
- markku

On Thursday, March 22, 2018 at 8:13:58 PM UTC, Markku-Juhani O. Saarinen wrote:

Hi,

There is a single point on p. 17 of the HILA5 specification which erroneously claims IND-CCA security. With much speculation about this this was shown not to be correct in [1]. Every other point in the paper talks of IND-CPA. The original academic paper [2] has never mentioned IND-CCA.

Furthermore the [1] clearly states that "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."

So there will be a three letter tweak to the specification (and appropriate reference), which of course has zero effect on implementations and test vectors. Creating a variant with Fujisaki–Okamoto as suggested in [1] is not a bad idea, and will probably do that only if selected for the next round, not to affect first round evaluation too much.

I have since left ARM and once I get a Cambridge PO Box address (towards end of the month), I will be posting a corrected version with new contact details. See you all in Ft. Lauderdale next month!

References:


Cheers.
- markku

Dr. Markku-Juhani O. Saarinen <mjos@iki.fi>

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov. Visit this group at https://groups.google.com/a/list.nist.gov/group/pqc-forum/.