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

--

From: Markku-Juhani O. Saarinen <mjos.crypto@gmail.com>
Sent: Thursday, March 22, 2018 4:46 PM
To: pqc-forum
Subject: [pqc-forum] Re: HILA5 v1.0 is of course IND-CPA

Hi.

Actually that is more like a single letter error in a single spot of the specification (page 17). Corrected version now up at at https://github.com/mjosaarinen/hila5/raw/master/Supporting_Documentation/hila5spec.pdf

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:
>
> [1] Daniel J. Bernstein, Leon Groot Bruinderink, Tanja Lange, and Lorenz Panny, ``HILA5 pindakaas: On the CCA security of lattice-based encryption with error correction.'' IACR ePrint 2017/1214, December 2017. URL: https://eprint.iacr.org/2017/1214.
>
> [2] Markku-Juhani O. Saarinen. ``HILA5: On reliability, reconciliation, and error correction for Ring-LWE encryption.'' In Carlisle Adams and Jan Camenisch, editors, Selected Areas in
> Cryptography – SAC 2017. 24th International Conference, Ottawa, ON, Canada, August 16 - 18, 2017, volume 10719 of Lecture Notes in Computer Science, pages 192–212. Springer, 2018.
> doi:10.1007/978-3-319-72565-9_10.
>
> Cheers.
> - markku
>
> Dr. Markku-Juhani O. Saarinen <mjos@iki.fi>

From: Markku-Juhani O. Saarinen <mjos.crypto@gmail.com>
Sent: Saturday, March 31, 2018 12:04 PM
To: pqc-forum
Subject: [pqc-forum] Re: HILA5 v1.0 is of course IND-CPA [OFFICIAL COMMENT]

Hi,

Version 1.02 of spec now up at the same
address https://github.com/mjosaarinen/hila5/raw/master/Supporting_Documentation/hila5spec.pdf

Updated:
1. Got a brand new postal address,
2. Footnote on p. 17 now more clearly promises a Fujisaki-Okamoto IND-CCA variant in the future.

Code and test vectors unchanged.

Cheers,
- markku

On Thursday, March 22, 2018 at 8:46:27 PM UTC, Markku-Juhani O. Saarinen wrote:

> Hi.
>
> Actually that is more like a single letter error in a single spot of the specification (page 17). Corrected version now up at at https://github.com/mjosaarinen/hila5/raw/master/Supporting_Documentation/hila5spec.pdf
>
> 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:
> >
> > [1] Daniel J. Bernstein, Leon Groot Bruinderink, Tanja Lange, and Lorenz Panny, ``HILA5 pindakaas: On the CCA security of lattice-based encryption with error correction.'' IACR ePrint 2017/1214, December 2017.
> > URL: https://eprint.iacr.org/2017/1214.
> >
> > [2] Markku-Juhani O. Saarinen. ``HILA5: On reliability, reconciliation, and error correction for Ring-LWE encryption.'' In Carlisle Adams and Jan Camenisch, editors, Selected Areas in Cryptography – SAC 2017. 24th International Conference, Ottawa, ON, Canada, August 16 - 18, 2017, volume 10719 of Lecture Notes in Computer Science, pages 192–212. Springer, 2018.

From: Leon Groot Bruinderink <leon.gb90@gmail.com>
Sent: Monday, April 09, 2018 3:32 PM
To: pqc-forum
Subject: [pqc-forum] Re: HILA5 v1.0 is of course IND-CPA

Follow Up Flag: Follow up
Flag Status: Flagged

Dear Markku,

Our paper https://eprint.iacr.org/2017/1214 showed that HILA5 is not secure against chosen-ciphertext attacks, even if AEAD is used for the user-specified message encrypted under the HILA5 session key. This led to withdrawal of an IND-CCA security claim for HILA5.

However, there are six documents with non-withdrawn claims of "active security" for HILA5, such as the following:

> For active security we suggest that K is used as keying material for an AEAD (Authenticated Encryption with Associated Data) [Rog02] scheme such as AES256-GCM [Dwo07, FIP01] or Keyak [BDP+16] in order to protect message integrity.

We would like to know what "active security" means in this quote, if it does not have the usual meaning of chosen-ciphertext security (either IND-CCA1 or IND-CCA2, both of which are broken by our attack).

The six documents mentioned above are the following.

1. The original version of the HILA5 paper, currently available here:

   https://eprint.iacr.org/2017/424.pdf

2. The Springer version of the paper (unfortunately paywalled):

   https://link.springer.com/chapter/10.1007/978-3-319-72565-9_10

3. The original HILA5 specification submitted to NIST (hila5spec.pdf in the submission package).

4. Specification version 1.01 dated 22 March 2018.

5. Specification version 1.02 dated 31 March 2018.

6. Specification version "1.020180404134100" dated 4 April 2018, currently available here:

   https://github.com/mjosaarinen/hila5/raw/master/Supporting_Documentation/hila5spec.pdf

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

Op donderdag 22 maart 2018 16:13:58 UTC-4 schreef Markku-Juhani O. Saarinen:

> Hi,

From: Markku-Juhani O. Saarinen <mjos.crypto@gmail.com>
Sent: Monday, April 09, 2018 5:32 PM
To: pqc-forum
Subject: [pqc-forum] Re: HILA5 v1.0 is of course IND-CPA

Follow Up Flag: Follow up
Flag Status: Flagged

On Monday, April 9, 2018 at 8:31:30 PM UTC+1, Leon Groot Bruinderink wrote:

> Dear Markku,
>
> We would like to know what "active security" means in this quote, if it does not have the usual meaning of chosen-ciphertext security (either IND-CCA1 or IND-CCA2, both of which are broken by our attack).

I appreciate that you have shown that a particular version of HILA5 is not IND-CCA (but only IND-CPA) but I fail to see the point with such semantic speculation.

Active security is an admittedly vague term used in various versions of the paper to motivate things like additional hashing of the final shared secret (with public key and ciphertext), which does stop certain, but not all, active attacks. I specifically did not want to claim IND-CCA1 or IND-CCA2.

Furthermore, thank you for checking six versions of the document, including an academic write-up, and verifying that none of which claim IND-CCA, apart from a single typo in the submission document in a paragraph that actually discusses IND-CPA.

As mentioned, I will update HILA5 in later stage to include a version that is IND-CCA (and claims to be IND-CCA).

Cheers,
- markku

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