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