Dear all:
There is an error in the reference implementation of Lotus.
In the implementation of tagextract, as defined in section 2.4.7 of the specs, the only two bits of stage $S_{18}$ used are also discarded.
As a result, the last 2 bits of all tags are always zero. This can be easily checked with the KATs, as the last nibble of each ciphertext is always one of \{0,4,8,C\}.
Best regards

Miguel Montes
Dear all,

We thank Miguel for pointing out the bug in the reference implementation of WAGE.

The bug was in the `wage_gentag` function and the details are as follow.
- **Incorrect version**: `tmp tag[18] = ((state[18]>>2)&(0x03));`
- **Correct version**: `tmp tag[18] = ((state[18]<<2)&(0x60));`

We have fixed the bug in the reference implementation code (also attached here).

Please note that:
1) The test vector given in Appendix A of the specification file is not affected by the bug.
2) **There are no changes in the specification of WAGE.**

Thanks and Regards,
The WAGE Team

On Sat, Apr 27, 2019 at 4:16 PM Miguel Montes <miguel.montes@gmail.com> wrote:

Dear all:
There is an error in the reference implementation of Lotus.
In the implementation of `tagextract`, as defined in section 2.4.7 of the specs, the only two bits of stage $S_{18}$ used are also discarded.
As a result, the last 2 bits of all tags are always zero. This can be easily checked with the KATs, as the last nibble of each ciphertext is always one of {0,4,8,C}.
Best regards

Miguel Montes

--
To unsubscribe from this group, send email to lwc-forum+unsubscribe@list.nist.gov
Visit this group at https://groups.google.com/a/list.nist.gov/d/forum/lwc-forum

---
You received this message because you are subscribed to the Google Groups "lwc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to lwc-forum+unsubscribe@list.nist.gov.

--
To unsubscribe from this group, send email to lwc-forum+unsubscribe@list.nist.gov
Visit this group at https://groups.google.com/a/list.nist.gov/d/forum/lwc-forum