From: lwc-forum@list.nist.gov on behalf of Ashwin Jha <letterstoashwin@gmail.com>
Sent: Friday, September 18, 2020 10:27 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov; avik chakraborti; Nilanjan Datta; Ashwin Jha; cuauhtemoc.mancillas83@gmail.com; Mridul Nandi; sasaki.yu@lab.ntt.co.jp
Subject: [lwc-forum] ROUND 2 OFFICIAL COMMENT: ESTATE
Attachments: estate_v1.tar.gz

Dear all,

This is to report two minor bug fixes in the reference implementation of ESTATE.

Bug 1 -- In encrypt.c, mac function: a return statement is missing in the if(adlen==0 && ptlen==0) block.

Fix --- Add a return statement at the end of the above mentioned if block.

Bug 2 -- In tweaes-128.c, add_round_tweak function: the tweak value is XORed to the first two columns of the AES state.

This bug was identified by one of the anonymous reviewers of IACR ToSC 2020 Special Issue 1. We thank the reviewer for pointing this bug to us.

Fix --- XOR tweak value to the first two rows of the AES state.

Please find attached the updated reference implementation with the above mentioned fixes.

Note that this does not introduce any changes in the specification of ESTATE.

Regards,
Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-Lopez, Mridul Nandi, Yu Sasaki
ESTATE Team