From: Raghvendra Rohit <iraghvendrarohit@gmail.com>
Sent: Monday, November 25, 2019 4:18 PM
To: lightweight-crypto
Cc: rsrohit@uwaterloo.ca
Subject: ROUND 2 OFFICIAL COMMENT: ACE

Dear NIST and LWC community,

It was brought to our attention by Rama Hardy that the minimum number of active Sboxes corresponding to different examined permutations of ACE's branches which is reported in Table 4.1 is not accurate. We found that the chosen permutation, (3,2,0,4,1), in ACE results in

- Case 1: **19** active Sboxes if we consider input and output differences in any state word (**we reported 21**). Hence, the minimum number of active Sboxes for up to 16 rounds is given by [0, 1, 2, 3, 4, 6, 7, 8, 10, 11, 13, 14, 15, 16, 18, 19].
- Case 2: **21** active Sboxes if we consider differences in the rate parts only, i.e., both input and output differences in words A and C, only (**we reported 21**). Hence, the minimum number of active Sboxes for up to 16 rounds is given by [None, None, 4, 6, 6, 8, 10, 10, 12, 14, 14, 16, 17, 18, 20, 21].

Note that the miscalculations in Case 1 **do not affect** the claimed security when ACE is used in a mode (AE, hash), an adversary can only inject and cancel the difference at rate positions which is Case 2. Further, the rate positions within these words are non-consecutive and the adversary can only control 64 bits of rate, while differential trail probability is bounded by 2^{-15.8 * 21}. So, there may exist a distinguisher for the permutation (here differential distinguisher with probability 2^{-15.8 * 19}) which is not directly exploitable in a mode.

We would like to emphasize that this minor error in our analysis neither affects the claimed security of ACE nor changes its specification.

We would like to thank Rama Hardy for his thorough analysis which led to this note.

Thanks,
ACE Team