

Changelog to SPIX (Round 2 Candidate)

Riham AlTawy, Guang Gong, Morgan He,
Kalikinkar Mandal, and Raghvendra Rohit

September 27, 2019

The following changes are done in Round 2 SPIX submission.

1. Fixed the bug related to associated data (AD) processing in the reference implementation. More specifically, the earlier version of the code (in `proc_ad` function) did not process the padded block when AD length is a multiple of 8. Note that the fixed code has been already posted on LWC forum (OFFICIAL COMMENT: SPIX, dated June 5 2019). Moreover, comments are added in software codes to make them more comprehensible.
2. Added microcontroller code with the submission package.
3. Fixed some minor typos in the document.
4. Updated the contact details of corresponding author and link of SPIX website in coversheet.