Gimli: modifications for round 2

20190927

The Gimli algorithms (encryption, decryption, and hashing), the Gimli formal specification in hacspec, the Gimli test vectors, and the Gimli implementations are unchanged.

The following changes have been made to the documentation for the second round:

- We fixed an error in the description of the differential propagation of Gimli. This error was not present in the model used for computing the differential trails and therefore does not affect the cryptanalytic results for Gimli. We would like to thank Rusydi Makarim for pointing this out to us.
- We fixed an error in the algorithmic description of the AEAD decryption mode and some erroneous indices in the AEAD description. We would like to thank Michael Tempelmeier and Patrick Karl for pointing this out to us.
- We added a summary of the Liu–Isobe–Meier paper attacking Gimli-Hash reduced to the first 5 of 24 rounds, and attacking Gimli-Hash reduced to the last 4 rounds. We would like to thank Fukang Liu, Takanori Isobe, and Willi Meier for this analysis.