Change_log of mixFeed

Designers/Submitters:
Bishwajit Chakraborty - Indian Statistical Institute, Kolkata
Mridul Nandi - Indian Statistical Institute, Kolkata, India
bishu.math.ynwa@gmail.com
mridul.nandi@gmail.com

September 21, 2019

1. in Lines 8,10,11 of mixFeed_enc : all Y's have been renamed to T.

2. in Lines 20, 22,23 of mixFeed_dec: all Y,T's have been renamed to T'.

3. in Line 5 of Fmt : m is corrected to n.

4. in Line 7: proc_txt(K1,Y0,D,d_D) is changed to proc_txt(K1,Y0,D,d_D,dir) (the argument dir was missing in the subroutine proc_txt before).

5. in Line 10 of proc_txt: Feed(Yi,D+_i) is changed to Feed(Yi,D+i,dir).

6. In the caption of Table 2, "and" is corrected to "or".

7. In Section 3 namely "Security of mixFeed", the last line before section 3.1 claiming about the nonce misuse security of mixFeed, is removed.

8. Section 5-8 giving a security proof of mixFeed added.

9. In Appendix, the test-vectors for AES'128/128 were duplicates and input,key were not written properly including intermediate 0's. Hence we could not verify the correctness of it. New test vectors added.

10. An appendix named Relevant figures for mixFeed is added.

There is no corrections to be made in the Pseudocode of the algorithm. All the corrections are required either due to typo's or due to wrongly representing the in-chain and out-chain variables of the block ciphers. No change is required in the reference implementation.