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 $\mathsf{mixFeed}_{[\mathsf{E}]}.\mathsf{enc}$: all Y's have been renamed to T.

2. in **Lines 20, 22,23** of $\mathsf{mixFeed}_{[\mathsf{E}]}.\mathsf{dec}$: all Y, T's have been renamed to T'.

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

4. in **Line 7**: $\mathsf{proc\_txt}(K_1, Y_0, D, \delta_D)$ is changed to $\mathsf{proc\_txt}(K_1, Y_0, D, \delta_D, dir)$ (the argument dir was missing in the subroutine proc_txt before).

5. in **Line 10** of proc_txt: $\mathsf{Feed}(Y_i, D_i, +)$ is changed to $\mathsf{Feed}(Y_i, D_i, dir)$.

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 imtermediate 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**.