# Errata 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

April 28, 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 $\mathsf{Fmt}$ : $m$ 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 $\mathsf{proc\_txt}$ before).
5. in **Line 10** of $\mathsf{proc\_txt}$: $\mathsf{Feed}(Y_i, D_i, +)$ is changed to $\mathsf{Feed}(Y_i, D_i, dir)$.

There is no conceptual corrections to be made in the Pseudocode of the algorithm. All these changes 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**. For the sake of completeness we rewrite the pseudocode below:

1: **function** $\textsc{mixFeed}_{[\mathsf{E}]}.\mathsf{enc}(K, N, A, M)$
2: $((a, \delta_A), (m, \delta_M)) \leftarrow \mathsf{Fmt}(A, M)$
3: **if** $a = 0, m = 0$ **then**
4: $(T, *) \leftarrow \mathsf{E}_K(N \| 0^6 10)$
5: **return** $(\lambda, T)$
6: **else if** $a = 0$ **then** $(K_N, *) \leftarrow \mathsf{E}_K(N \| 0^7 1)$
7: **else** $(K_N, *) \leftarrow \mathsf{E}_K(N \| 0^8)$
8: $(T, K) \leftarrow \mathsf{E}_{K_N}(N \| 0^8)$
9: $C \leftarrow \lambda$
10: **if** $a \neq 0$ **then** $(*, T, K) \leftarrow \mathsf{proc\_txt}(T, K, A, \delta_A, +)$
11: **if** $m \neq 0$ **then** $(C, T, *) \leftarrow \mathsf{proc\_txt}(T, K, M, \delta_M, +)$
12: **return** $(C, T)$

13: **function** $\textsc{mixFeed}_{[\mathsf{E}]}.\mathsf{dec}(K, N, A, C, T)$
14: $((a, \delta_A), (m, \delta_C)) \leftarrow \mathsf{Fmt}(A, C)$
15: **if** $a = 0, m = 0$ **then**
16: $(T', *) \leftarrow \mathsf{E}_K(N \| 0^6 10)$
17: **return** $(T = T')? \top : \bot$
18: **else if** $a = 0$ **then** $(K_N, *) \leftarrow \mathsf{E}_K(N \| 0^7 1)$
19: **else** $(K_N, *) \leftarrow \mathsf{E}_K(N \| 0^8)$
20: $(T', K) \leftarrow \mathsf{E}_{K_N}(N \| 0^8)$
21: $M \leftarrow \lambda$
22: **if** $a \neq 0$ **then** $(*, T', K) \leftarrow \mathsf{proc\_txt}(T', K, A, \delta_A, +)$
23: **if** $m \neq 0$ **then** $(M, T', *) \leftarrow \mathsf{proc\_txt}(T', K, C, \delta_C, -)$
24: **if** $T \neq T'$ **then**
25: **return** $\bot$
26: **else**
27: **return** $(M, \top)$

1: **function** $\mathsf{Fmt}(A, M)$
2: $(A_{a-1}, \ldots, A_0) \xleftarrow{n} A$
3: $(M_{m-1}, \ldots, M_0) \xleftarrow{n} M$
4: $\delta_A \leftarrow (n \mid |A_{a-1}|)$ & $(m = 0)? \ 12 : 4 : 14 : 6$
5: $\delta_M \leftarrow (n \mid |M_{m-1}|)? \ 13 : 15$
6: **return** $((a, \delta_A), (m, \delta_M))$

7: **function** $\mathsf{proc\_txt}(K_1, Y_0, D, \delta_D, dir)$
8: $(D_{d-1}, \ldots, D_0) \xleftarrow{n} D$
9: **for** $i = 0$ **to** $d - 1$ **do**
10: $(X_{i+1}, D'_i) \leftarrow \mathsf{Feed}(Y_i, D_i, dir)$
11: $(Y_{i+1}, K_{i+2}) \leftarrow \mathsf{E}_{K_{i+1}}(X_{i+1})$
12: $X_{d+1} \leftarrow Y_d \oplus 0^{n-4} \| \delta_D$
13: $(Y_{d+1}, K_{d+2}) \leftarrow \mathsf{E}_{K_{d+1}}(X_{d+1})$
14: **return** $(D', Y_{d+1}, K_{d+2})$

15: **function** $\mathsf{Feed}(Y, D, \mathrm{dir})$
16: $D' \leftarrow D \oplus \lfloor Y \rfloor_{|D|}$
17: **if** dir $=$ " $+$ " **then**
18: $B \leftarrow \lceil \mathsf{pad}(D') \rceil_{n/2} \| \lfloor \mathsf{pad}(D) \rfloor_{n/2}$
19: **if** dir $=$ " $-$ " **then**
20: $B \leftarrow \lceil \mathsf{pad}(D) \rceil_{n/2} \| \lfloor \mathsf{pad}(D') \rfloor_{n/2}$
21: $X \leftarrow B \oplus Y$
22: **return** $(X, D')$