Change_log of ORANGE

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 20, 2019

In spec_orange.pdf: We make the following corrections on the specification document. No corresponding change is required in the reference implementations.

1. ORANGE-Zest$_{[P]}$.enc **line 9**: return value $(C, \mathsf{proc\_tg}(U))$ and not $\mathsf{proc\_tg}(U)$.

2. function ORANGISH **line 21**: There is no α multiplication in Hash. So $Z \leftarrow \mathsf{proc\_hash}(X, (A_{d-1}\| \ldots \|, A_0), 0, 0)$ and not $Z \leftarrow \mathsf{proc\_hash}(X, (A_{d-1}\| \ldots \|, A_0), 1, 1)$.

3. function proc_txt **line 37**: return value is (D', U_d) and not (D', U_a).

4. function ORANGE-Zest$_{[P]}$.dec :
   (a) **line 5** : $a = 0$ is changed to $a = 0, m \neq 0$.
   (b) **line 8** : $N\|K$ has been corrected to $K\|N$.
   (c) **line 9** : $m \neq 0$ is changed to $a \neq 0, m \neq 0$.

5. function mult **line 32** : return value is $\alpha^c \cdot V^b \parallel V^t$ and not $V^t \parallel \alpha^c \cdot V^b$.

6. "and" is repaced by "or" in the caption of Table 2.

7. Section 5 is moved to subsection 4.3. Hence the changes in section numbers of the subsequent sections follow.

8. The security proof for a modified version of ORANGE-Zest is added in Section 8 and Section 9 .

9. Appendix A has been moved to section 7. Consequently Appendix B is now Appendix A.

10. Some new References have been added.

In crypto_aead/orangezestv2/ref/orangemodule.h: The primitive polynomial *alpha_128* was getting reset to x^{128} instead of $x^{128} + x^7 + x^2 + x + 1$. (in **lines 84-90** of orangemodule.h). This is corrected by using an **else** argument in **line 88** of orangemodule.h. The test vectors have been changed accordingly in the specification.