# Clarifications in the specification of ELmD v1.0

Nilanjan Datta and Mridul Nandi

Indian Statistical Institute, Kolkata, India.

In this short note, we clarify some issues, that were not properly mentioned in the specification of ELmD v1.0.

## 1 ELmD Tagged Ciphertext Generation when $\mathsf{t} = 0$.

The tagged ciphertext algorithm is given for non-zero $\mathsf{t}$ and we mentioned that, for $\mathsf{t} = 0$, no intermediate tag is generated i.e. $T$ is empty. Note that, the definition of $C[i]$ is given as : $C[i] = CC[i] \oplus 3^2 \cdot 2^{i-1+\lfloor \frac{i-1}{\mathsf{t}} \rfloor} \cdot L$. Although we meant, $\lfloor \frac{i-1}{\mathsf{t}} \rfloor = 0$ for $\mathsf{t} = 0$ but as it was not properly mentioned in the specification, it might lead to some confusion. Here, we provide the ELmD algorithm for $\mathsf{t} = 0$ more formally, to remove any confusion :

$$
\begin{aligned}
W[0] &= IV \\
M[l+1] &= \oplus_{i=1}^{l} M[i] \\
MM[i] &= M[i] \oplus 2^{i-1} \cdot L \quad \text{for } i = 1 \text{ to } (l-1) \\
MM[l] &= \begin{cases} M[l] \oplus 2^{l-1} \cdot L & \text{if } |M^*[l]| = 128 \\ M[l] \oplus 7 \cdot 2^{l-2} \cdot L & \text{else} \end{cases} \\
MM[l+1] &= \begin{cases} M[l+1] \oplus 2^{l} \cdot L & \text{if } |M^*[l]| = 128 \\ M[l+1] \oplus 7 \cdot 2^{l-1} \cdot L & \text{else} \end{cases} \\
X[i] &= E_K(MM[i]) \quad \text{for } i = 1 \text{ to } (l+1) \\
(Y[i], W[i]) &= \rho(X[i], W[i-1]) \quad \text{for } i = 1 \text{ to } (l+1) \\
CC[i] &= E_K^{-1}(Y[i]) \quad \text{for } i = 1 \text{ to } l \\
C[i] &= CC[i] \oplus 3^2 \cdot 2^{i-1} \cdot L \quad \text{for } i = 1 \text{ to } l \\
CC[l+1] &= E_K^{-1}(Y[l+1] \oplus 1) \\
C[l+1] &= CC[l+1] \oplus 3^2 \cdot 2^{l} \cdot L
\end{aligned}
$$

## 2 Description of $\mathsf{AES}^{\mathsf{r}}$.

For $\mathsf{r}$ round AES encyption, $\mathsf{r}$ rounds of encryptions are used. In the specification, we have mentioned it as $\mathsf{r} + 1$ rounds of encryption, which was a typo. In the recommended parameter set, we have used $\mathsf{AES}^{10}$ and $\mathsf{AES}^{5}$. $\mathsf{AES}^{10}$ is the standard 10 round AES-encryption, where the mix column operation is skipped in the last round. For $\mathsf{AES}^{5}$, we will have the last round mix-column operation - hence have 5 full round encryptions. In general, when $\mathsf{r} < 10$, $\mathsf{AES}^{\mathsf{r}}$, we will have the last round mix-column operation - hence have $\mathsf{r}$ full round encryption.