Proposal of ELmD v2.1

Nilanjan Datta and Mridul Nandi

Indian Statistical Institute, Kolkata
nilanjan_isi_jrf@yahoo.com, mridul.nandi@gmail.com

Abstract. In this short document, we propose the specification of ELmD v2.1 which has a small modification from the version ELmD v2.0. Very recently, we observe that due to the small changes made in the ELmD v2.0, the scheme have online privacy upto the last but one block, in nonce-misuse scenario. To achieve the privacy for the last block, we made a small change in the masking procedure. This change ensures a stronger security of ELmD - online privacy upto the last but one block and full privacy for the last block.

1 Proposed Modification

We propose a small Modification in the masking mechanism. Here, we update the masking value for the plaintext by 7 and 7^2 instead of 2 and 7 respectively. More formally, we define $MM[l]$ and $MM[l+1]$ as :

$$MM[l] = \begin{cases} M[l] \oplus 7 \cdot 2^{l-2} \cdot L & \text{if } |M^*[l]| = 128 \\ M[l] \oplus 7^2 \cdot 2^{l-2} \cdot L & \text{else} \end{cases}$$

$$MM[l+1] = \begin{cases} M[l+1] \oplus 7 \cdot 2^{l-1} \cdot L & \text{if } |M^*[l]| = 128 \\ M[l+1] \oplus 7^2 \cdot 2^{l-1} \cdot L & \text{else} \end{cases}$$

Brief Explanation of the Modification. For nonce-misuse scenario, ELmD v2.0 has online privacy upto the last but one block but doesn't have security for the last block. This new masking ensures online privacy upto the last but one block and full privacy for the last block. In particular, if we consider two messages with one being prefix of another, then the last ciphertext block for the small message will not depend on any ciphertext blocks of the long message.