Change Log

1. We have added a chapter on the hardware results of LOTUS-AEAD and LOCUS-AEAD (see Chapter 6).

2. We have also fixed a minor bug in the reference implementation of TweGIFT-64_LOTUS-AEAD.

   In "encrypt.c", at line 96:
   Previous version: "`xor_bytes(nonced_key, nonce, CRYPTO_ABYTES);`"
   Correct version: "`xor_bytes(nonced_key, nonce, CRYPTO_NPUBBYTES);`"

   We thank Miguel Montes for reporting this bug. Note that, this is purely an implementation bug and does not require any change in the design.