Changelog

[September 26, 2019]

1. On page 6:
   Previous version: "COMET-128_AES-128/128: This version sets $n = 128$ and uses *the 8-round variant of* AES-128/128 as the underlying block cipher."
   Current version: "COMET-128_AES-128/128: This version sets $n = 128$ and uses AES-128/128 as the underlying block cipher."
   Reason for change: "the 8-round variant of" was a typo. that remained there from an earlier draft of the specification file. We use full 10 rounds of AES-128/128 as is evident from the reference implementation as well as the "Security Claims" section.

2. On page 7, just before the "Design Rationale" section:
   Previous version: "Several test vectors corresponding to the four submissions are available in appendix ??."
   Current version: This line has been removed.
   Reason for change: This line was again from an earlier draft of the specification file. In the final specification file we did not provide test vectors (as they are already given in the KAT file). So we removed this line.