Changes to the Round 2 TinyJAMBU Submission Paper

Designers and Submitters: Hongjun Wu and Tao Huang

Division of Mathematical Sciences
Nanyang Technological University
wuhongjun@gmail.com

27 September 2019

In the Round 2 submission, there is no change to the codes and test vectors of TinyJAMBU. There is no change to the specification of TinyJAMBU. The following changes are made to the security analysis of TinyJAMBU.

1. In Section 6.2.1 Differential Properties of the Keyed Permutation P_n
   (a) In Table 6.1, added the Type 1 differential probability for 512 rounds.
   (b) In Table 6.2, added the Type 2 differential probability for 512 rounds.
   (c) In Table 6.3, improved the Type 3 differential probability for 384 rounds.
   (d) Added Type 4 differential and the Table 6.4
2. In Section 6.2.2 Linear Properties of the Keyed Permutation P_n
   (a) In Table 6.5, added the linear bias for 512 rounds.
3. In Section 6.3.2 Forgery attacks on plaintext/ciphertext
   (a) In the second and third paragraph of this section, updated the forgery attack result
4. In Section 6.4.1 Differential cryptanalysis
   (a) A new paragraph is added as the first paragraph of this section. The differential attack using nonce is analysed in this paragraph.
   (b) In the second paragraph of this section, updated the differential attack using plaintext/ciphertext

5. In Section 6.4.2 Linear cryptanalysis

   (a) In the second paragraph of this section, updated the linear attack using plaintext/ciphertext

6. In Section 7.2 Software Performance

   (a) The software performance data are updated in Table 7.2 and Table 7.3.