Cryptography Theory and Practice, Fourth Edition

Errata

January 30, 2019

Thanks to Morteza Esmaeili and Tamir Tassa for bringing errors to our attention.

1. On page 121, line 11 from the bottom of the page,

   $$r_{16} \oplus 01$$

   should be replaced by

   $$r_{16} \oplus 01 \oplus LB(y_0), \text{ where } LB(y_0) \text{ denotes the last byte of } y_0.$$

   Similarly, on page 122, line 3,

   $$r_{15} \oplus 02$$

   should be replaced by

   $$r_{15} \oplus 02 \oplus SLB(y_0), \text{ where } SLB(y_0) \text{ denotes the second last byte of } y_0.$$

2. On page 128, in the matrix A, the third and fourth rows are redundant. One of them should be deleted.

   Also, the displayed equation

   $$0 = f(z_1, z_2, z_3, z_0 + z_1)$$

   should be replaced by

   $$1 = f(z_1, z_2, z_3, z_0 + z_1)$$