Errata — RadioGatún, a belt-and-mill hash function

Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche

2007-03-09

This document lists the known errors in the paper RadioGatún, *a belt-and-mill hash function* presented at the Second Cryptographic Hash Workshop, Santa Barbara, August 24-25, 2006.

- Section 6.1. The third line of Algorithm 3 should be

  $$B[i] = b[i - 1 \bmod 13]$$

  (instead of $i + 1$). The reference code is correct, however.

- Section 7. In the first sentence of the section, the words "latter" and "former" should be exchanged.