From: hash-forum@nist.gov on behalf of Jean-Philippe Aumasson [jeanphilippe.aumasson@gmail.com]
Sent: Monday, May 25, 2009 4:49 AM
To: Multiple recipients of list
Subject: OFFICIAL COMMENT: BLAKE

We have been informed of some discrepancies in the C code of BLAKE, mostly related to the treatment of messages of length not a multiple of 8 bits. The revised C code is available on BLAKE's website:
http://www.131002.net/blake/

Neither security nor speed is affected.

The bugs were found by Daniel Otte, who implemented certain SHA-3 candidates in AVR microcontroller. See his website:
http://www.das-labor.org/wiki/AVR-Crypto-Lib/en