BLAKE round 3 modifications

Jean-Philippe Aumasson Luca Henzen Willi Meier Raphael C.-W. Phan

The modifications of the BLAKE hash function submission to NIST are the following:

- The number of rounds for the 224- and 256-bit digest versions is changed from 10 to 14.
- The number of rounds for the 384- and 512-bit digest versions is changed from 14 to 16.
- The BLAKE instances are renamed from BLAKE-28, BLAKE-32, BLAKE-48, and BLAKE-64 to, respectively, BLAKE-224, BLAKE-256, BLAKE-384, and BLAKE-512.