
From: hash-forum@nist.gov on behalf of Jean-Philippe Aumasson
[jeanphilippe.aumasson@gmail.com]
Sent: Thursday, December 16, 2010 6:15 AM
To: Multiple recipients of list
Subject: OFFICIAL COMMENT: BLAKE name change

The four instances of BLAKE, as tweaked for the final, are renamed BLAKE-224, BLAKE-256, BLAKE-384, and BLAKE-512 (instead of BLAKE-28, BLAKE-32, BLAKE-48, and BLAKE-64). This change will avoid confusion when looking at previous speed benchmarks.

The BLAKE website (<http://131002.net/blake/>) has been redesigned and updated with new supporting documentation and implementations according to the tweak and to the renaming.