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.

Caswell, Sara J.

From:	Shilpa Chauhan <cshilpa24@gmail.com>
Sent:	Thursday, May 24, 2012 11:58 AM
To:	internal-hash
Cc:	HASH-FORUM
Subject:	OFFICIAL COMMENT: BLAKE (Round 3)

BLAKE-512 on ARM7TDMI can hash at about 233 cycles/byte, on Cortex M3 can hash at about 248 cycles/byte and on Cortex A9 can hash at speed of about 140 cycles/byte.

These results were calculated on IAR Embedded Workbench in Simulator mode.

Starting from 1 byte to 1100 byte there were 50 input sets. The graph between the number of bytes and cycles/byte depicts that with increasing input size, the running time of all the tree algorithms was reduced.

--
Thanks and Regards
Shilpa Chauhan