From: D. J. Bernstein [djb@cr.yp.to]
Sent: Wednesday, July 15, 2009 8:21 PM
To: hash-function@nist.gov
Cc: hash-forum@nist.gov
Subject: OFFICIAL COMMENT: CubeHash

At the First SHA-3 Candidate Conference, NIST asked whether submissions would be secure if they were tuned to be as fast as SHA-2 on the NIST reference platform, a Core 2 Duo.

My original recommendations for CubeHash parameters weighted security much more highly than speed. In light of NIST's comments I have written a document "CubeHash parameter tweak: 16 times faster" issuing new recommendations for the CubeHash parameters, reaching speeds between
11.47 cycles/byte and 14.07 cycles/byte on various Core 2 Duo CPUs in both 32-bit mode and 64-bit mode:

http://cubehash.cr.yp.to/submission/tweak.pdf

The CubeHash algorithm itself is unchanged, and cryptanalysts are faced with the same spectrum of reduced-security targets as challenges. If CubeHash is allowed into the second round then I would like this tweak to be considered as part of the submission.

---D. J. Bernstein
Research Professor, Computer Science, University of Illinois at Chicago