From: hash-forum@nist.gov on behalf of Burr, William E. [william.burr@nist.gov]
Sent: Friday, July 24, 2009 11:02 AM
To: Multiple recipients of list
Subject: Announcement of Second Round SHA-3 Candidates

NIST received 64 SHA-3 candidate hash function submissions and accepted 51 first round candidates as meeting our minimum acceptance criteria. We have now selected the following 14 second round candidates to continue in the competition:

BLAKE
Blue Midnight Wish
CubeHash
ECHO
Fugue
Grøstl
Hamsi
JH
Keccak
Luffa
Shabal
SHAvite-3
SIMD
Skein

We were pleased by the amount and quality of the cryptanalysis we received on the first round candidates, and more than a little amazed by the ingenuity of some of the attacks. We thank all the submitters, those who provided analysis, those who provided valuable implementation performance data (particularly e-Bash, and the papers dealing with the effects of the AES round instruction, FPGA implementations, and working store requirements of the algorithms). We were also pleased and grateful (although not surprised) for the graceful and forthright manner with which several of the submitters took bad news, and confirmed attacks, or recognized the shortcomings of their submission.

In selecting this set of second round candidates we tried to include only algorithms that we thought had a chance of being selected as SHA-3. We were willing to extrapolate higher performance for conservative designs with apparently large safety factors, but comparatively unforgiving of aggressive designs that were broken, or nearly broken during the course of the review. We were more willing to accept disquieting properties of the hash function if the designer had apparently anticipated them, than if they were discovered during the review period, even if there were apparent fixes. We were generally alarmed by attacks on compression functions that seemed unanticipated by the submitters.

There are still some details of a few of the second round candidates that concern us. We will shortly post a statement describing each of the second round candidates, the factors that we liked about the submission and identifying any lingering concerns that we have. Submitters of the second round candidates are invited to tweak their submissions to improve them if they wish, fix any inconsistencies, problems or shortcomings in the specification or source code, and submit them to us by Sept. 15, 2009.

Information about the second round candidate algorithms will be available at:
http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/index.html.

Best regards,

Bill Burr