Subject: OFFICIAL COMMENT: Fugue
From: Charanjit Jutla <csjutla@us.ibm.com>
Date: Thu, 18 Dec 2008 17:36:43 -0500
To: hash-function@nist.gov
CC: hash-forum@nist.gov

1. We have updated figures for Fugue-256's performance on X86-64.

An optimized ANSI C implementation (with NIST API included) runs at 60 Mbytes/sec on a 2GHZ machine (E5335), i.e. 33 cycles/byte. Brian Gladman's highly optimized SHA-256 runs at 84 MB/sec on the same machine. Our implementation would be 25% faster if the L1 cache was twice as large. On 128 bit platforms, we expect 100% speed improvement. The submitted code (which is not optimized) also runs at 55 MB/sec. We are not yet submitting the new optimized code, but will change the numbers (according to 55 MB/sec impl) in the PDF document being re-submitted to NIST.

2. There were lots of typos in the PDF document submitted to NIST, including some minor technical issues in the security proofs sections, in particular section 10. They have all been fixed and will be resubmitted in the fresh PDF document. There is NO CHANGE in the SPECIFICATION section (not even a typo). While it is being updated at NIST, if you are reading the document you should read the one on IBM's website:

http://domino.research.ibm.com/comm/research_projects.nsf/pages/fugue.index.html

Thanks,

Charanjit Jutla

From: Charanjit Jutla [csjutla@us.ibm.com]
Sent: Thursday, May 07, 2009 2:21 PM
To: hash-function@nist.gov
Subject: OFFICIAL COMMENT: Fugue (Speed Update)

Follow Up Flag: Follow up
Flag Status: Red

Here is an updated speed estimate for the code provided earlier to NIST (referred to as optimized 32-bit code, and this same code is used for both
32 and 64 bit measurements):

Hardware: T7700 (Core 2) 2.4 GHz (90nm)
O/S: 32-bit Windows
Compiler: Intel C++ v 11.(-O2)
Message Size: 10k bytes
Language: ANSI C

Fugue-256 : 26.7 cycles/byte
Fugue-512: 53 cycles/byte

Hardware: Same as above
O/S: Linux 64 bit
Compiler: GCC 4.2 (-O2)
Message Size: 10K bytes.
Language: ANSI C

Fugue -256:   25 cycles/byte
Fugue-512 :   50 cycles/byte

SSE-2 Estimate : on 32 bit core -2 (90nm) machine: 23 cycles/byte
on 32-bit core -2 (45nm) machine: 20
cycles/byte

-Charanjit Jutla