Subject: OFFICIAL COMMENT: Skein
From: Bruce Schneier <schneier@schneier.com>
Date: Thu, 19 Feb 2009 10:28:26 -0500
To: Multiple recipients of list <hash-forum@nist.gov>

In our Skein paper, we reference an unpublished paper detailing Skein's proofs of security.

We have posted a draft of that paper on the Skein website:

http://www.skein-hash.info/sites/default/files/skein-proofs.pdf

Bruce

I had sent this message to the forum in January, but we wanted to make sure it was an “official” comment on the NIST web site, so here it is again:

Just a note that we now have Skein-512 running at 20 clks/byte on a Core 2 Duo CPU in 32-bit code, using the SSE2 instruction set and registers. Because the SSE2 registers are in size, this approach can actually perform two different Threefish/Skein blocks in parallel (i.e., ~10 clks/byte!), which could be quite useful for counter mode or tree has Thanks to Randall Farmer for developing this code.

In 64-bit CPU code, straight C is still considerably faster than using SSE2.

See the Skein web page for details: http://www.skein-hash.info/

Doug Whiting

This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information which is protected from disclosure. Any unauthorized review, use, disclosure or distribution by any means is prohibited. If you are not the intended recipient, please contact the sender by reply email or at (408) 399-3500 and destroy all copies of the original message.

From: hash-forum@nist.gov on behalf of Jon Callas [jon@pgpeng.com]
Sent: Monday, May 11, 2009 12:49 PM
To: Multiple recipients of list
Subject: OFFICIAL COMMENT: Skein

Our proofs paper is finally up at:

<http://www.skein-hash.info/sites/default/files/skein-proofs.pdf>

Jon

```
--
Jon Callas
CTO, CSO
PGP Corporation         Tel: +1 (650) 319-9016
200 Jefferson Drive     Fax: +1 (650) 319-9001
Menlo Park, CA 94025    PGP: ed15 5bdf cd41 adfc 00f3
USA                          28b6 52bf 5a46 bc98 e63d
```