
From: hash-forum@nist.gov on behalf of Chang, Shu-jen H. [shu-jen.chang@nist.gov]
Sent: Thursday, October 15, 2009 11:52 AM
To: Multiple recipients of list
Subject: FW: OFFICIAL COMMENT: Fugue (Round 2)

FYI

The official comment shown below was not sent to hash-forum. I'd like to inform you that we have received an update package of Fugue and have posted it on the NIST site as an **update**. We don't plan to accept future updates unless for a very good reason. Submitters are advised to send OFFICIAL COMMENT and post corrections on their web site.

Regards,
Shu-jen

From: Charanjit Jutla [mailto:csjutla@us.ibm.com]
Sent: Friday, October 02, 2009 4:50 PM
To: hash-function@nist.gov
Subject: OFFICIAL COMMENT: Fugue (Round 2)

Dear all,

1. Stefan Tillich (of Graz University of Technology) has found a bug in the __implementation__ of Fugue's padding. In particular, for messages which are not of byte-multiple length, the implementation erroneously zeroes the last incomplete byte. The bug is in all implementations, including reference, and the way the KAT files were generated. As a result, the KATs for non-byte-confirming messages are wrong.

2. We will correct the implementation, and post new KAT files and the implementations on the IBM site next week. The link will be posted here again. We will see how/when/if it can be incorporated into NIST's posted version.

3. To emphasize, the bug is NOT in the Fugue padding specification, but in the implementation. The specification remains unchanged.

4. The implementations submitted to eBASH remain unchanged, as they are for byte length messages only.

5. We appreciate the fact that Stefan contacted us first, rather than posting directly on the forum.

6. For those who are curious, the bug is not in Fugue.c, but in the wrapper file SHA3api_ref.c. Line 62 reads:

10/20/2009

```
memset ((uint8*)state->Partial+((state->TotalBits&31)/8), 0, need/8);
```

It should instead be:

```
memset ((uint8*)state->Partial+(((state->TotalBits&31)+7)/8), 0, need/8);
```

7. Thanks for your patience,

The Fugue Team