From: Gaëtan Leurent [gaetan.leurent@ens.fr]
Sent: Tuesday, February 23, 2010 10:21 AM
To: hash-function@nist.gov
Cc: hash-forum@nist.gov
Subject: OFFICIAL COMMENT: SIMD (Round 2)

A typo in the specification of SIMD has been reported by Luca Henzen and Thomas Pornin.

Page 22, algorithme 1, ligne 32, the constant 24 should actually be 25.
This constant is used as a rotation in the compression part.
A fixed version of the specification is available at the following address:
  http://www.di.ens.fr/~leurent/files/SIMD.pdf

The code was using the correct value, so the test vector are not affected by this typo.

The rationale behind using 25 instead of 24 is that we want to use a relatively small set of rotation amount to allow for more efficient implementations. In particular, these offset needs to be inside registers on some architecture and it helps if they are used multiple times before changing to a new set of rotations.

Sincerely,

--
Gaëtan Leurent