DEPARTMENT OF ELECTRICAL ENGINEERING ESAT/SCD-COSIC,
KATHOLIEKE UNIVERSITEIT LEUVEN
KASTEELPARK ARENBERG 10/2446
B-3001 HEVERLEE, BELGIUM.

KATHOLIEKE
UNIVERSITEIT
LEUVEN

Larry Bassham
NIST
100 Bureau Drive
MS 8930
Gaithersburg, MD 20899–8930

LEUVEN, 2009–01–15
ENCL Updated Specification document: "The LANE Hash Function"

List of Changes for Hash Algorithm Submission: LANE

Dear Sir,

Please find attached to this letter the updated version of the documentation of the LANE hash function, our proposal to the NIST SHA-3 competition. There are no changes to the specification or implementations of LANE, just some very minor changes to the documentation.

A list of changes is given below.

1. Some minor typing errors and typographical errors were corrected.
2. In the first sentence of Section 2.6 on page 16, "... also includes the message length n" was corrected to read "... also includes the message length l".
3. In Table 4.1 on page 30, the entries for 6, 7 and 8 rounds of LANE-512 in were updated after supplemental computer search.
4. The text in Section 4.2.2 on page 30 was also updated to reflect these new, improved numbers.
5. Also Section 4.2.4 on page 32 was updated, as it builds on the data from Table 4.1. In particular, equation (4.8) was updated.

Sincerely

Sebastiaan Indesteege

SEBASTIAAN INDESTEEGE
TEL. +32 16 32 10 49 FAX +32 16 32 19 69
E-mail: sebastiaan.indesteege@esat.kuleuven.be

ASSOCIATIE K.U.LEUVEN