

MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LABORATORY

Ronald L. Rivest

The Stata Center, Room 32-G692

32 Vassar Street, Cambridge, MA USA 02139-4307

+1.617.253.5880 fax: +1.617.258.8682 rivest@mit.edu



October 24, 2008

Ms. Shu-jen Chang

Information Technology Laboratory

Attention: Hash Algorithm Submissions

100 Bureau Drive-Stop 8930

National Institute of Standards and Technology

Gaithersburg, MD 20899-8930

Dear Ms. Chang –

This is the required “Cover Sheet” for our submission of the algorithm “MD6” for the NIST SHA-3 competition.

Name of the submitted algorithm:

MD6

Principal submitter’s name:

Ronald L. Rivest

Principal submitter’s email:

rivest@mit.edu

Principal submitter’s phone:

617-253-5880

Principal submitter’s fax:

617-258-8682

Principal submitter’s organization:

Massachusetts Institute of Technology

Principal submitter’s postal address:

Room G692
Computer Science and Artificial Intelligence Laboratory, MIT
32 Vassar Street
Cambridge, MA 02139

Name(s) of auxiliary submitters:

Benjamin Agre
Daniel V. Bailey
Christopher Crutchfield
Yevgeniy Dodis
Kermin Elliott Fleming
Asif Khan
Jayant Krishnamurthy
Yuncheng Lin
Leonid Reyzin
Emily Shen
James Sukha
Drew Sutherland
Eran Tromer
Yiqun Lisa Yin

Name of the algorithm inventor(s)/developer(s):

Ronald L. Rivest

Name of the owner, if any, of the algorithm (normally expected to be the same as the submitter):

Ronald L. Rivest

(optional) Backup point of contact:

Eran Tromer, CSAIL, MIT

Sincerely,

A handwritten signature in black ink that reads "Ronald L. Rivest". The signature is written in a cursive style with a large, stylized 'R' and 'L'.

Ronald L. Rivest
Andrew and Edna Viterbi Professor