Call for Papers for the Second SHA-3 Candidate Conference
Santa Barbara, CA
August 23-24, 2010
Submission deadline: May 10, 2010 (Conference without proceedings)

The SHA-3 competition has entered the second round, in which 14 second-round candidate algorithms are being considered for SHA-3. NIST plans to host a Second SHA-3 Candidate Conference in August, 2010 to discuss various aspects of these candidates, and to obtain valuable feedback for the selection of the finalists soon after the conference.

NIST is soliciting research and discussion papers, surveys, presentations, case studies, panel proposals, and participation from all interested parties, including researchers, system architects, implementers, vendors, and users. NIST will post the accepted papers and presentations on the conference web site after the conference; however, no formal conference proceedings will be published. NIST encourages the submission of presentations and reports on preliminary work that participants plan to publish elsewhere. To avoid the possible duplication of papers accepted for this conference and for Crypto and CHES 2010, which are held consecutively, submissions will NOT be considered for this conference if they are substantially similar to the submissions accepted for Crypto 2010 and CHES 2010.

Topics for submissions should include, but are not limited to, the following:

- Cryptanalysis of candidates, including cryptanalysis of weakened or toy versions;
- Analysis of relative performance or resource requirements for some or all candidates;
- Statistical or other automated analyses or comparisons of candidates;
- Substantial improvements in implementation of candidates;
- Improved analysis or proofs of properties of candidates, even when this doesn't lead to any attack; and
- Proposed criteria to be used for selecting the finalists.

Deadlines:

- **Submission Deadline: May 10, 2010**
- **Authors Notified: June 18, 2010**
- **Final Version Deadline: July 23, 2010**

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x 11 inches). Submitted papers must not exceed 15 pages (single space, with 1 inch margins using a 10 pt or larger font). Proposals for panels should be no longer than five pages, and should include possible panelists and an indication of which panelists have confirmed their participation.

Please submit the following information to **hash-function@nist.gov**

- Name, affiliation, email, phone number, postal address for the primary submitter
- First name, last name, and affiliation of each co-submitter
- The finished paper, presentation, or panel proposal in PDF format as an attachment.

All submissions will be acknowledged.

General information about the conference, including the registration and accommodation information will be available at the conference website: **http://www.nist.gov/hash-competition**