**Call for Papers for the Third SHA-3 Candidate Conference**
Washington, DC (Details to be announced and posted on http://www.nist.gov/hash-competition)
March 22-23, 2012 (in conjunction with FSE, March 19-21, 2012)
**Submission deadline: ~~Nov. 4, 2011~~ Extended to Nov. 25, 2011 (Conference without proceedings)**

The SHA-3 Cryptographic Hash Algorithm Competition has entered the third and final round, in which five finalist algorithms are being considered for the final SHA-3 selection. NIST plans to host the Third SHA-3 Candidate Conference in March 2012 to discuss the security, performance, evaluation metrics and various aspects of the finalists, and to solicit public feedback before it selects the winning algorithm as SHA-3 later in 2012.

NIST is soliciting research and discussion papers, surveys, presentations, case studies, panel proposals, and participation from all interested parties, including researchers, implementers, protocol designers, system architects, 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 FSE 2012, submissions will NOT be considered for this conference if they are substantially similar to the submissions accepted for FSE 2012.

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

- Cryptanalysis of the candidates, including cryptanalysis of weakened or toy versions;
- Side channel analysis of the candidates;
- Analysis of relative performance or resource requirements for the candidates;
- Evaluation metrics to facilitate candidate analysis and comparison;
- Statistical or other automated analyses or comparisons of the candidates;
- Substantial improvements in the implementation of the candidates;
- Improved analysis or proofs of security properties of the candidates, even when this doesn't lead to any attack; and
- Other suggestions to be considered for the SHA-3 selection.

**Deadlines:**

- **Submission Deadline: ~~Nov. 4, 2011~~ Extended to Nov. 25, 2011**
- **Authors Notification: ~~Jan. 20, 2012~~ Extended to Jan. 27, 2012**
- **Final Version Deadline: Feb. 17, 2012**

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x 11 inches). Submission papers must not exceed 15 pages (single spaced, with 1 inch margins using a 10 pt or larger font). Proposals for presentations or panels should be no longer than five pages; panel proposals 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 conference location, registration and accommodation information will be available at the conference website: **http://www.nist.gov/hash-competition**.