SHA-3 2014 Workshop (workshop without proceedings)
Santa Barbara, CA
(Revised) Date: August 22, 2014 (Immediately after Crypto 2014)

DEADLINES

- **Submission Deadline: April 12, 2014**
- **Authors Notified: June 13, 2014**
- **Workshop Version Deadline: July 21, 2014**

NIST announced KECCAK as the winner of the SHA-3 Cryptographic Hash Algorithm Competition in October 2012 after a five-year selection process that got a tremendous amount of response from the cryptographic community. NIST is in the process of writing KECCAK up formally as a FIPS; in addition, NIST is planning to standardize other uses of SHA-3, including authenticated encryption and pseudo random function, along with developing a general standard for tree hashing. However, there are still many important research questions remaining surrounding SHA-3 and its variants and applications.

NIST is planning to host a SHA-3 Workshop on August 22, immediately following Crypto 2014, in Santa Barbara. NIST hopes this workshop will continue the vigorous participation of the cryptographic research community that made the SHA-3 Competition a success. The goal of the workshop is for the community to help NIST get a better understanding of SHA-3 and its possible applications, with particular focus on additional modes of operation for SHA-3 that might be worth standardizing in the future. Although the workshop is focusing on SHA-3, NIST is also interested in new results on the SHA-2 family of hash functions.

NIST is soliciting research, surveys, discussion papers, presentations, case studies, panel proposals, and participation from all interested parties, including researchers, system architects, vendors, and users. NIST will post the accepted papers and presentations on the workshop web site; however, no formal workshop proceedings will be published. NIST encourages presentations and reports on preliminary work that participants plan to publish elsewhere. To avoid the possible duplication of papers accepted for this workshop and Crypto 2014, submissions will NOT be considered for this workshop if they are substantially similar to the submissions accepted for Crypto 2014 or for other workshops held at UCSB in conjunction with Crypto 2014.

WORKSHOP TOPICS

Workshop topics include, but are not limited to:

- Cryptanalysis of SHA-3 or closely related variants that might shed light on SHA-3's ultimate security
- Bounds on differential trails and correlations in the SHA-3 permutations
- Experimental results on side-channel analysis of SHA-3 implementations
- Improved proofs of security for SHA-3
- Security of SHA-3 variants using smaller permutations
- Performance and implementation impact of using smaller permutations
- Alternative modes of operation for the SHA-3 permutations, and
- Any new results on SHA-2.

INSTRUCTIONS FOR SUBMITTERS

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x 11 inches). Paper submissions must not exceed 15 pages (single space, with 1" 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.

Submissions should be sent to **hash-function@nist.gov** with the following information:

- Name, affiliation and email address for the primary contact author
- Name and affiliation of each co-author
- The finished paper, presentation, or panel proposal in PDF as an attachment.

General information about the workshop including the registration and accommodation information will be available at the workshop website: http://www.nist.gov/hash-function.