NIST SHA3 Workshop*

Aug 22-23, Immediately after Crypto 2014
Santa Barbara, CA

* Workshop without proceedings

http://csrc.nist.gov/groups/ST/hash/sha-3/Aug2014/SHA3-aug2014-call-for-papers.pdf

What's to Talk About?

- Cryptanalysis of SHA-3

- ...or closely related variants

- 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

- Much more

http://csrc.nist.gov/groups/ST/hash/sha-3/Aug2014/SHA3-aug2014-call-for-papers.pdf

Important Dates

- Conference: August 22-23, 2014 (Immediately after Crypto 2014)

- Submission Deadline: April 12, 2014

- Authors Notified: June 13, 2014

- Workshop Version Deadline: July 21, 2014

http://csrc.nist.gov/groups/ST/hash/sha-3/Aug2014/SHA3-aug2014-call-for-papers.pdf