SHA-3 2014 Workshop

August 22, 2014

University of California, Santa Barbara [Corwin Pavilion]

Friday August 22, 2014	
8:30	**Registration Opens**
9:00 – 9:10 (10 minutes)	**Opening Remarks** Donna F. Dodson, *ITL Associate Director, Chief Cybersecurity Advisor, and Director of the National Cybersecurity Center of Excellence*
9:10 – 9:55 (45 minutes)	**Session I: SHA-3 Standard, XOFs** (20 minutes each) **Session Chair:** Lily Chen, *NIST* 1. **SHA-3 Standard: Overview, Status, Public Comment** *Presented by*: Morris Dworkin, *NIST* 2. **Uses of XOFs** *Presented by*: Ray Perlner, *NIST*
9:55 – 10:40 (45 minutes)	**Session II: Security Analysis** (20 minutes each) **Session Chair:** Meltem Sönmez Turan, *NIST* **1.** **Practical Complexity Cube Attacks on Round-Reduced Keccak Sponge Function** [**paper**] *Presented by*: Itai Dinur, *École normale supérieure* **2.** **1st and 2nd Preimage Attacks on 7, 8 and 9 Rounds of KECCAK-224, 256, 384, 512** [**paper**] *Presented by*: Donghoon Chang, *Indraprastha Institute of Information Technology, Delhi*
10:40 – 11:00 (20 minutes)	**Coffee Break**
11:00 – 11:25 (25 minutes)	**Session III: Implementations** **Session Chair:** Bill Burr, *NIST* **1.** **Shrinking KECCAK Hardware Implementations** [**paper**] *Presented by*: Bernhard Jungk, *easycore GmbH*
11:25 – 11:50 (25 minutes)	**Session IV: Invited Talk by the KECCAK Team** **Introduced by:** Bill Burr, *NIST* **1.** **The KECCAK Code Package** *Presented by*: Gilles Van Assche, *STMicroelectronics*

11:50 – 12:35 (45 minutes)	**Session V: Hash Modes** (20 minutes each) **Session Chair:** Andrew Regenscheid, *NIST* **1.** **Using the KECCAK Technology for Authenticated Encryption: KETJE, KEYAK and More** *Presented by*: Joan Daemen, *STMicroelectronics* **2.** ***i*SHAKE: Incremental Hashing with SHAKE128 and SHAKE256 for the Zettabyte Era** **[paper]** *Presented by*: Danilo Gligoroski, *Norwegian University of Science and Technology*
12:35 – 13:50 (75 minutes)	**Lunch** ***De La Guerra Dining Commons***
13:50 – 15:05 (75 minutes)	**Session VI: Parallelizable Hashing** (20 minutes for the presentation, followed by the panel discussion) **Session Chair:** John Kelsey, *NIST* **1.** **Parallelized Hashing via j-lanes and j-pointers Tree Modes, with Applications to SHA-256** [paper] *Presented by*: Shay Gueron, *University of Haifa and Intel Corporation* **2.** **Panel on Parallelizable Hashing – Overview & Discussion** *Facilitator*: John Kelsey, *NIST* ***Panelists:*** Scott Fluhrer, *Cisco Systems* Kris Gaj, *George Mason University* Shay Gueron, *University of Haifa and Intel Corporation* Gilles Van Assche, *STMicroelectronics*
15:05 – 15:25 (20 minutes)	**Coffee Break**
15:25 – 16:15 (50 minutes)	**Session VII: NIST Plans** (15 minutes each) **Session Chair:** Rene Peralta, *NIST* **1.** **Special Publication on Authenticated Encryption** *Presented by*: Meltem Sönmez Turan, *NIST* **2.** **Special Publication on KMAC** *Presented by*: Ray Perlner, *NIST* **3.** **Domain Extensions** *Presented by*: Morris Dworkin, *NIST*
16:15 – 16:55 (40 minutes)	**Session VIII: Open Discussion** **Session Chair:** John Kelsey, *NIST*
16:55 – 17:05 (10 minutes)	**Closing Remarks & Adjourn** Lily Chen, *NIST*