Random Bit Generation Workshop

May 2-3, 2016

Agenda

Monday, May 2, 2016	
9:00 – 9:10	**Opening Remarks** Welcome and workshop purpose, Matthew Scholl, NIST
9:10 – 10:30	**Session I -** Chair: Meltem Sonmez Turan 1. *High level overview of SP 800-90B,* John Kelsey, NIST 2. *High level overview of SP 800-90C,* Elaine Barker, NIST
10:30-11:00	**Break** (refreshments available for purchase in the cafeteria)
11:00 – 12:30	**Session II -** Chair: Elaine Barker 1. *Entropy Estimation for Non-IID Sources,* Kerry McKay, NIST 2. *Conditioning functions,* John Kelsey, NIST 3. *IID testing,* Meltem Sonmez Turan, NIST
12:30-13:30	**Lunch Break**
1:30 – 2:30	**Session III -** Chair: Apostol Vassilev 1. *Entropy Estimation on the Basis of a Stochastic Model,* Werner Schindler, BSI Germany, Speaker: Peter Birkner 2. *Estimating Min-entropy for large output spaces*, Darryl Buller, Aaron Kaufer, NSA
2:30 – 3:00	**Break** (refreshments available for purchase in the cafeteria)
3:00 -4:00	**Session IV -** Chair: Kerry McKay 1. *Entropy as a Service,* Apostol Vassilev, NIST 2. *Canary Numbers Design for Light-weight Online Testability of True Random Number Generators,* Vladimir Rozic, Bohan Yang, Nele Mentens and Ingrid Verbauwhede, COSIC

Workshop Website: http://go.usa.gov/cvXt3

Presentations and abstracts will be online following the workshop.

Tuesday, May 3, 2016	
9:00 – 10:30	**Session V -** Chair: Vincent M. Boyle 1. *New approach for miniaturization of Quantum Random Number Generator*, Jeong Woon Choi and Seung Hwan Kwak, SK Telecom, Korea 2. *Progress towards Quantum-based Random Number Generation using Entangled Photons*, Joshua C. Bienfang, Peter Bierhorst, Alan Mink and Stephen Jordan, Paulina Kuo, Scott Glancy, S. Nam, K. Shalm, M. Stevens, T. Gerrits, R. Mirin, V. Verma, A. Lita, C. Hodge, NIST 3. *Trust, and public entropy: a unicorn hunt*, Arjen K. Lenstra and Benjamin Wesolowski, EPFL IC LACAL, Switzerland
10:30-11:00	**Break** (refreshments available for purchase in the cafeteria)
11:00 – 12:30	**Session VI -** Chair: Meltem Sonmez Turan 1. *Minimizing false negative and false positive errors on entropy health tests*, Scott Fluhrer, Cisco Systems 2. *Sources of randomness in digital devices and their testability*, Viktor Fischer, CNRS, France 3. *The impact of digitization on the entropy generation rates of physical sources of randomness*, Joseph D. Hart, Thomas E. Murphy, and Rajarshi Roy, UMD
12:30-13:30	**Lunch Break**
1:30 – 3:30	**Session VII** – Chair: John Kelsey Open discussions Closing

Workshop Website: http://go.usa.gov/cvXt3
Presentations and abstracts will be online following the workshop.