NORTHERN ARIZONA UNIVERSITY

Department of Mathematics and Statistics

COLLOQUIUM
Tuesday, September 6th, 2015
4:00 – 5:00 pm, Adel Mathematics Bldg., Room 164
(refreshments at 3:45)

Dr. Bertrand Cambou

Professor of Practice, Cybersecurity
School of Informatics, Computing, and Cyber Systems
NAU

Design of a true random number generator with a XOR data compiler

Abstract: We are describing how the level of randomness of ternary cells generated from memory arrays can be foundational for the generation of TRNG when coupled with a XOR data compiler. We are specifically presenting two complementary elements: i) the design of a XOR data compiler which process the data available from ternary cells to enhance randomness; and ii) how a combinational probability model based on Bernoulli function allows the quantification of the level of randomness of the TRNG. Deviations from absolute randomness of these TRNG in terms of probability to be non-random can be lower than 10-10 which is accepted as non-detectable from existing and computers of the foreseeable future.

Algebra Combinatorics Geometry and Topology (ACGT) Seminar meets every Tuesday, 12:45 – 1:45 pm, AMB 164. Michael Falk begins speaking this Tuesday.
Applied Math Seminar (AMS) meets every Thursdays, 12:45 – 1:45 pm, AMB 164, as announced. Jeffrey Covington speaks this Thursday.

Friday Afternoon Undergraduate Mathematics Seminar (FAMUS) meets Fridays, 3pm, AMB 164.