NORTHERN ARIZONA UNIVERSITY

Department of Mathematics and Statistics

COLLOQUIUM
Tuesday, September 29th, 2015
4:00 – 5:00 pm, Adel Mathematics Bldg., Room 164
(refreshments at 3:45)

Bertrand Cambou
NAU

Design of cryptographic solutions

Abstract: Brief review of the symmetric and asymmetrical cryptography with the usage of the number theory. Presentation the following axis of research:

1. Physically Unclonable Functions (PUF), statistical analysis to extract error rates during authentication.
2. True Random Number Generator, randomness improvement.
3. Usage of lock up tables to accelerate cryptographic computations.

Algebra Combinatorics Geometry and Topology (ACGT) Seminar meets every Tuesday, 12:45 – 1:45 pm, AMB 164.

Applied Math Seminar (AMS) will meet occasionally on Thursdays, 12:45 – 1:45 pm, AMB 164, as announced.

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