Contribution ID: **1571** Type: **Oral**

Quality random number generator

Monday 28 October 2024 16:45 (15 minutes)

A good number of applications in physics (and not only) rely on random number generation for Monte Carlo purposed (or key distribution, and other tasks).

Most at hand random servers are hash function based, with carefully studied and tuned algorithms. Depending on complexity and quality of the samples produced, they can be very good quality like RANLUX (with 10^171 period), or faster, like the Mersenne Twister (x40 faster).

I present the implementation of a true-random multiplier, a code that relies on a finite set of true-random numbers from a physical source (in this case atmospheric noise, set of 0.2 M in the 0 … 9999 range). The code produces new numbers by combining any 2 random numbers in the list, at random distance between their list positions. The random offset relies on a shift register structure involving both the rand() hash and numbers from the list itself, thereby producing "non-repetitive repetitions" - i.e. the multiplier has no known period.

The tests of the multiplier are presented and they show good quality.

Primary author: DIMA, Maria (JINR - DLNP)

Co-authors: DIMA, Mihai-Tiberiu (JINR & Polytechnic Bucharest); ДИМА, Светлана; MIHAILESCU, Madalina (Hyperion University)

Presenter: DIMA, Maria (JINR - DLNP)

Session Classification: Mathematical Modelling and Computational Physics

Track Classification: Mathematical Modeling and Computational Physics