Statistical inference for oscillator-based random number generators

Maciej Skórski
University of Warsaw

Abstract

The aim of this talk is to overview the stochastic models of an elementary oscillator-based random number generator, building on the work of Baudet at al. (Journal of Cryptology, 2011), and present some new results that deepen the understanding of theoretical foundations and facilitate statistical inference.
The new results are based on the joint work with Nathalie Bochard and Viktor Fischer.

Keywords: statistical inference, oscillator-based true random number generators