1143-11-266 **Giacomo Micheli*** (giacomo.micheli@maths.ox.ac.uk). *Fractional Jumps.*

Constructing pseudorandom number generators (PRNG) has always been a task of great interest in applied areas and in particular in Cryptography. In this talk we produce PRNGs using Fractional Jumps of transitive projective maps. The concept of Fractional Jump intertwines the theory of projective automorphisms with the theory of polynomials over finite fields and analytic number theory. In turn this leads to competitive pseudorandom number generation. Furthermore, our theory covers entirely the theory of Inversive Congruential Generator (ICG) sequences. The sequences produced using our generators have the same discrepancy bound but improved computational complexity with respect to the classical ICG sequences. (Received August 16, 2018)