Abstract Submitted
for the MAR15 Meeting of
The American Physical Society

A new class of scalable parallel pseudorandom number generators based on Pohlig-Hellman exponentiation ciphers[1] PAUL BEALE, University of Colorado Boulder — We propose a new class of pseudorandom number generators based on Pohlig-Hellman exponentiation ciphers. The method generates uniform pseudorandom streams by encrypting simple sequences of short integer messages into ciphertexts by exponentiation modulo prime numbers. The advantages of the method are: the method is trivially parallelizable by parameterization with each pseudorandom number generator derived from an independent prime modulus, the method is fully scalable on massively parallel computing clusters due to the large number of primes available for each implementation, the seeding and initialization of the independent streams is simple, the method requires only a few integer multiply-mod operations per pseudorandom number, the state of each instance is defined by only a few integer values, the period of each instance is different, and the method passes a battery of intrastream and interstream correlation tests using up to 10^{13} pseudorandom numbers per test. We propose an implementation using 32-bit prime moduli with small exponents that require only a few 64-bit multiply-mod operations that can be executed directly in hardware. The 32-bit implementation we propose has millions of possible instances, all with periods greater than 10^{18}.

[1]Supported by NSF CNS-082179

Paul Beale
University of Colorado Boulder

Date submitted: 10 Nov 2014 Electronic form version 1.4