Non-Periodic Pseudo-Random Number Generator Using Sinai Billiards

Koranne, Advay (School: Catlin Gabel School)

A novel method of generating pseudo-random numbers (pRNG) using Hamiltonian-Dynamical systems is presented in this paper. Traditional pRNGs such as the Xorshift and the Mersenne Twister algorithm have known periods. However, by using Sinai Billiards which exhibit chaotic, non-periodic trajectories, I was able to create a non-periodic, pseudo-random sequence. The seed is represented as a coordinate and velocity pair on the boundary of the billiard, which is mapped using Birkhoff coordinate to ensure a dense map. A Sinai billiard is a polygon with a convex disk in the center, and by simulating the particle collisions with the boundary, I was able to generate a pseudo-random sequence. This model can be implemented in photonics on a processor chip with scatterers, mirrors, and a laser. Unlike other pRNGs, the photonic chip prevents the complete state of the particle from being known, resulting in a cryptographically secure system since the state of the generator is not stored in computer memory. Computer simulation of the proposed method demonstrates the viability of such an approach on a Monte-Carlo problem. According to my research, this is the only known method for a non-periodic, pseudo-random number generator which can be practically implemented.

Awards Won:

National Security Agency Research Directorate : Honorable Mention "Science of Security"