Pseudo-Random Number Generator using Sinai Billiards

Advay Koranne

Introduction

This research presents the first known **non-periodic pseudo-random number generation** (pRNG) technique which is practical and efficient. Pseudo-random numbers are a numbers which have random number characteristics, but produce the same sequence of numbers when given a initial seed. A practical method of generating pRNG using a simulation of a single particle billiard table is presented. By adding a disc in the center of the billiard (as seen in figure 1), it makes the particle have chaotic, but predicable behavior. This specific billiard table is called a Sinai Billiard [3]. By simulating this table one can use the non-periodic, chaotic, deterministic, characteristics of the system to generate a sequence of pseudo-random numbers. Yakov G. Sinai's proof of a particle moving in a billiard to be ergodic is the underlying basis of this research [3, 1] and a future implementation of this system using on-chip lasers is feasible.

Engineering Goal: To use Dynamical Billiards to create a pRNG with a infinite period for cryptography applications.

Model

Using Dynamical Billiards [2], I first created a hexagon (of unit side length) and computed the initial position and velocity such that the billiard particle has a periodic orbit (as shown in Figure 2(a)). If this system is used for random number generation, the sequence will be periodic, and thus insecure for **cryptographic applications.** Then I created a billiard table with a unit disk at the center (as shown in Figure 2(b)) with a particle on the boundary.
However, this method was not yielding an accurate value in the Mote-Carlo simulation. This was due to the fact that there were numerous areas where the particle was unable to reach, since the internal disk and the outside region between the hexagon and the square was not reachable. To solve this issue I parametrized the boundary from 0 to 1 using **Birkhoff coordinates [4]**. Then I time evolved the particle n number of collisions. For the computer simulations I have taken the $n = 60$ collision of the particle. Each collision is represented in Birkhoff coordinates, which by definition are dense in the set $[0, 1]$.

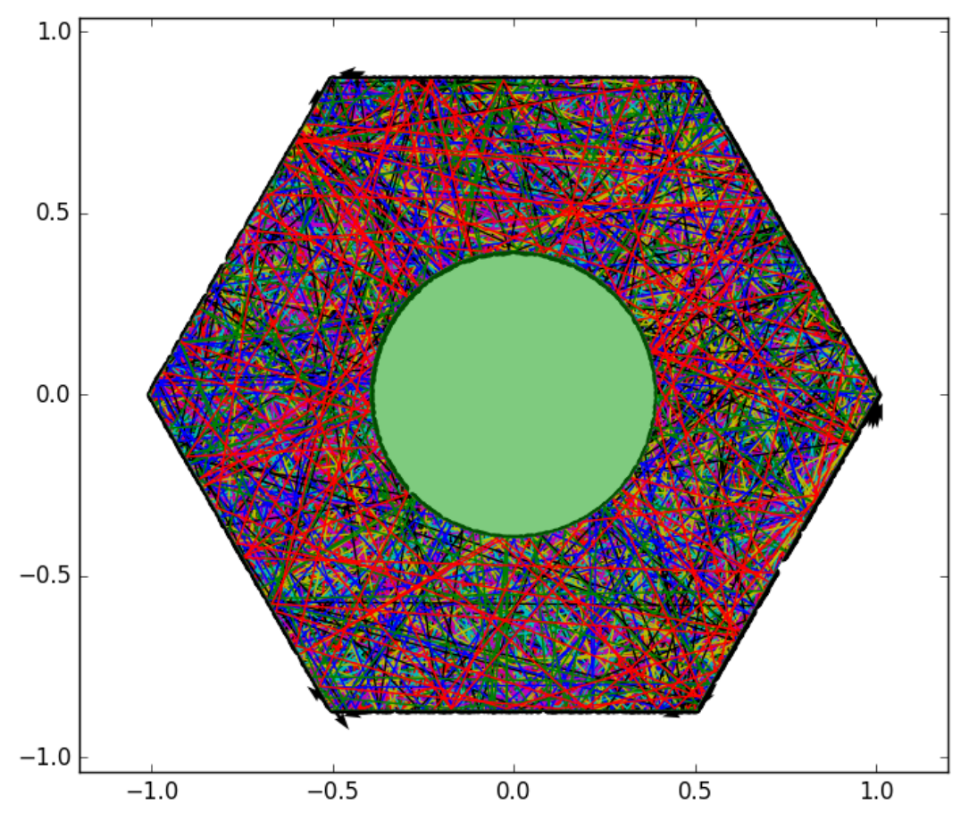

Fig. 1: **Dynamical Billiards (all images generated by Advay Koranne)**

Description of Sinai Billiard

A billiard is a Hamiltonian-dynamical system [3] where the system Ω is frictionless, and the particle has inelastic collisions. A Sinai billiard is a specific type off dynamical system in which there is a enclosed polygon with a convex disk in the center (as shown in Figure 2(b)).
Definitions

1. Billiards: A enclosed polygon (Ω) with smooth edges ($\partial\Omega \in C^1$), no pockets, and friction less surface over which a particle of unit velocity is evolved with inelastic collisions [1],
2. Ergodic: Same behavior averaged over time, as over space,
3. Dense: In a given area every point is explored and covered or RNG numbers inclusive between 0 and 1 are explored. You can prove something is dense if it is ergodic,
4. Pseudo Random: Exhibit statistically randomness while being generated by using a seed, same seed generates the same sequence,
5. Deterministic: Method is reproducible and time evolution is predictable given initial conditions.

Algorithm

Pseudo-random numbers have random number characteristics, however, when started with the same initial seed, they generate the same sequence. Prior to this research, no practical algorithm for generating non-periodic pseudo-random numbers was known. The seed in the proposed pRNG is the particle's initial location (u_0 in Birkhoff coordinate Γ) and velocity (θ, as $|v| = 1$). The parameterization of the location of the particle from $(x, y) \in \partial\Omega$ to Γ is one of the key ideas in my algorithm as that allows the map from $\Omega \to [0, 1]$ to be dense. Given this seed $(u_0, \theta) \in \Gamma \times 2\pi$ the time evolution $u(t), \theta(t)$ of the inelastic scattering generates the same sequence of numbers. It was one of the great discoveries of Sinai that although the system is integrable from initial conditions, almost all initial conditions exhibit non-periodic behavior, due to the scattering effect and positive Lyapunov exponent caused by the central disk. This non-periodicity makes our system future proof against attacks made by a much faster computer. Therefore, our pRNG can be used in cryptographic applications which have application life times spanning decades.

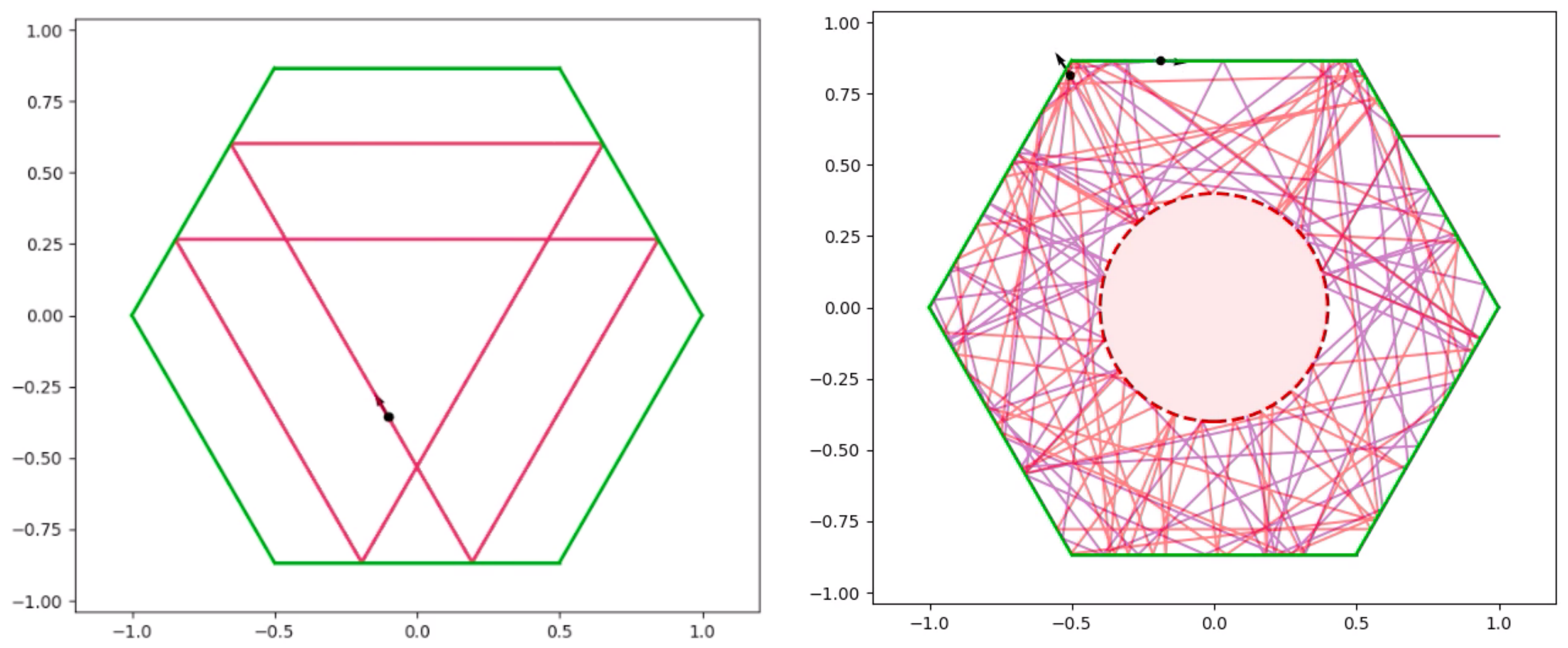

Fig. 2: Comparison of periodic path vs non-periodic path (all images generated by Advay Koranne)

Benefits of using Sinai Billiards to generate pRNG over other Algorithms

1. Fast (one number per clock cycle) especially when implemented on photonics due to short compute time,
2. State per pRNG is $u, \theta \in \Gamma \times 2\pi$: the same pRNG hardware can be shared to generate pRNGs for different applications. Each application only needs to store the particle location (in Γ) and velocity direction (as θ),
3. Large list of batched pRNG computed in relatively short compute steps (batched RNGs are used in cryptography),
4. Mathematically proved infinite period: all other pRNG have periods, even when the period is 2^{32}-bits, a fast computer in the future can break the cryptography.

Our algorithm is based on two fundamental mathematical principles, dynamical chaotic systems with positive Lyapunov exponents.

Characteristics of Chaos - Butterfly Effect

1. It must be sensitive to initial conditions (positive Lyapunov exponent),
2. It must be topologically mixing, and
3. it must have dense periodic orbits.

Lyapunov Exponent: $|u(t) - v(t)| \approx e^{\lambda t}|a(u_0 - v_0)|$

Lyapunov exponent λ tells us the rate of divergence of nearby trajectories. Consider two particles u, v with infinitesimally close initial positions u_0, v_0, and same θ. Since our system has a Lyapunov exponent which is positive (due to the central disk) it is highly sensitive to changes, therefore for any given distance M (less than the bounding diameter of the system), $\exists\ t$ such that $|u(t) - v(t)| > M$. This means that it is very hard to find the seed of a given sequence of numbers due to the exponential divergence of the paths.

Topological Mixing against other pRNG

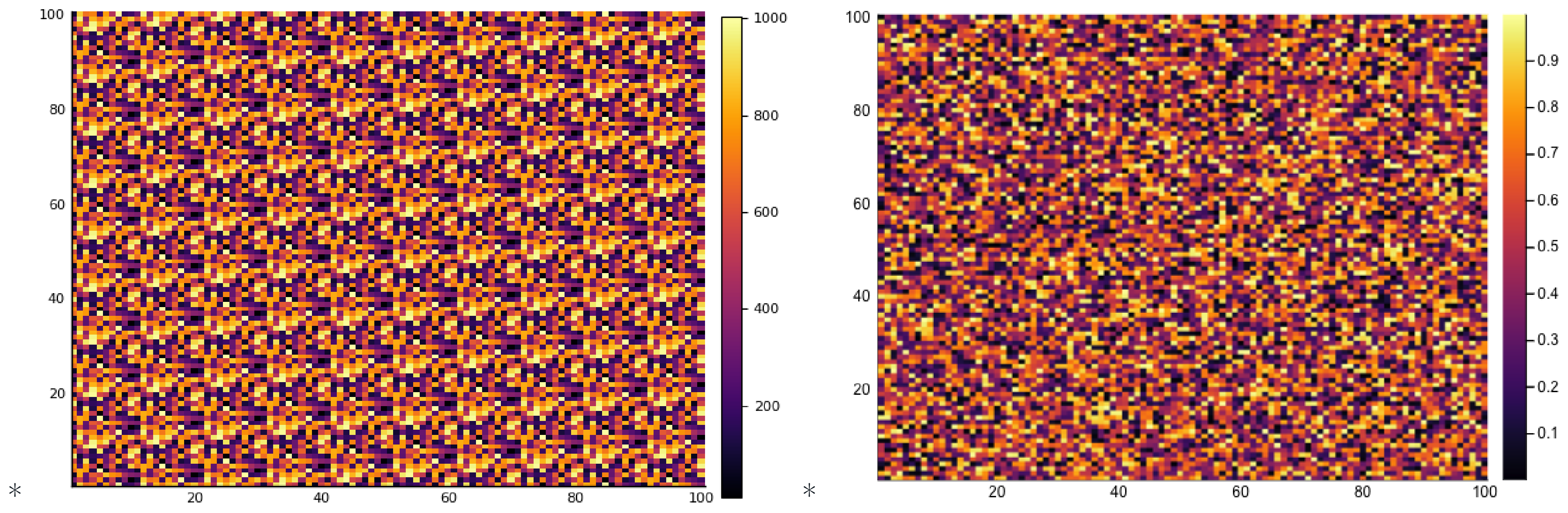

Fig. 3: Comparison of XOR based pRNG vs Dynamical Billiards pRNG (all images generated by Advay Koranne)

As shown above, the XOR-based pseudo-random number generator exhibits a particular periodic pattern which is visible. On the other hand, our proposed method has no periodicity. The lower the period the more insecure the data is thus it is crucial to have longer periods. The XOR based pRNG has a period of finite bit length, as compared to mine which has an infinite period.

Results

Table 1: Monte Carlo π Approximation

Monte Carlo π approximation					
Trials	Collisions	Julia rand()	% Error	Our Rand	% Error
1000	10	3.152	-0.3313	3.168	-0.8406
1000	60	3.148	-0.204	3.188	-1.4772
10000	10	3.122	0.6237	3.1328	0.2799
10000	60	3.1616	-0.6369	3.128	0.4327
100000	10	3.1274	0.4518	3.11848	0.7357
100000	60	3.1526	-0.3504	3.14552	-0.125

These results describe the Monte-Carlo π approximation. The estimated values show that the more trials that are present, my pRNG number generator is closer to the actual value of π compared to Julia's Mersenne Twister algorithm. This experiment validates the efficacy of the proposed algorithm for Monte-Carlo applications.

Table 2: Numerical simulation demonstrating topological mixing property of the proposed pRNG.

Topological Mixing		
Trial	2*Count (1 unit area)	Count (2 unit area)
0	2	0
1	198	208
2	11764	11708
3	210474	209473
4	1951816	1956444
5	12097318	12090185

To prove topological mixing I calculated the number of times the particle entered a phase space of measure 1 (in Birkhoff coordinate) and the number of times a particle enters another phase space of twice measure. These second value should be approximately 2 times as much as the first if the particle is ergodic, and this is confirmed in the numerical simulation as shown above.

Conclusion

Recent vulnerabilities in computer architecture have demonstrated the need for future proof cryptographic hardware. Pseudo-random number generators can alleviate most of the known problems, but generating non-periodic pRNG has been an unsolved problem. This research presents the first practical and efficient method of generating non-periodic pRNG. Numerical experiments with Monte-Carlo applications demonstrate the efficacy of the method. As the algorithm derives its non-periodicity from well established mathematical methods of dynamical billiards, the cryptographic analysis of the technique is directly established. Advances in photonics and on-chip laser generation also imply that simulation of particle in billiards of a chaotic system can be done efficiently in hardware using photons. That is why it is is crucial to come up with a security element which has infinite period. Though toady's pRNG have sufficiently long-periods ensuring security for data, as computer processing power doubles ever two years it is likely that future processors will be able to decrypt data easily. **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.** Future goals include passing NIST test and chip modelling. Understanding polygon unfolding in higher dimensions using dynamical billiards is a future research goals which may lead to faster methods for pRNG generation.

References

[1] Nikolai Chernov and Roberto Markarian. *Chaotic Billiards*. 127. American Mathematical Soc., 2006.

[2] George Datseris. "DynamicalBilliards.jl: An easy-to-use, modular and extendable Julia package for Dynamical Billiard systems in two dimensions." In: *The Journal of Open Source Software* 2.19 (Nov. 2017), p. 458. DOI: 10.21105/joss.00458. URL: https://doi.org/10.21105/joss.00458.

[3] Yakov G Sinai. "Dynamical systems with elastic reflections". In: *Russian Mathematical Surveys* 25.2 (1970), pp. 137–189. DOI: 10.1070/rm1970v025n02abeh003794.

[4] Serge Tabachnikov. *Geometry and billiards*. Vol. 30. American Mathematical Soc., 2005.