A Pseudo Random Number Generator Based on Chaotic Billiards

Khalid Charif, Ahmed Drissi, Zine El Abidine Guennoun
(Corresponding author: Khalid Charif)

Department of Mathematics, Mohamed V University in Rabat
No. 4, Avenue Ibn Battouta B. P. 1014 RP, Rabat, Morocco
(Email: Khalidcharif@gmail.com)
(Received Mar. 12, 2016; revised and accepted June 14 & July 17, 2016)

Abstract

The systems of chaotic billiards revealed a well developed chaotic behavior. Despite its good characteristics, these systems have not yet been applied to the cryptography; among the reasons is the difficulty of expressing the equation of particle motion in an explicit form. In this work, we took advantage the properties offered by the random walks and unpredictability of two particles moving in a chaotic billiard (Sinai Billiard) for the designing a new pseudo-random number generator. The results are subjected to an experimental study to test the randomness and the chaotic behavior of the generator. the key stream passed all the NIST statistical tests and the generator is highly sensitive for a bit change in the keys.

Keywords: Chaos, pseudo-random number generator, Sinai billiard

1 Introduction

The use of chaotic systems in cryptography has been well studied [17, 18, 19]. In fact there are similarities between the needs of cryptography and properties offered by the chaos. The algorithms based on chaos showed good performance for data encryption such as images, videos or audio data [1, 16, 20, 25]. Characterized by speed, reproducibility and simplicity of implementation, the PRNGs based on chaos took more attention. The first PRNG was proposed by Oishi and Inoue [21] in 1982, using the chaotic first order nonlinear differencial equations. After this article, several GNPAs were suggested. Generators have been proposed based on the logistic system in [2, 15, 23]. In [28], a generator based on the generalized Henon map. Using the Lorenz system, a new generator for the voice data encryption is designed in [1]. Chaotic standard system was applied in the conception of the generator in [22].

Our work focuses on an alternative approach based on the implementation of a system more concrete that has interesting chaotic properties, those are the systems of chaotic billiards in two dimensions [7]. They are among the classes of simple systems, which are still exploring chaos. The mathematical theory of billiards was introduced by Sinai in 1970 [26]. It is developed and evolved with remarkable speed to become a well grounded within the theory of dynamical systems theory and statistical mechanics. Several studies were devoted specifically to the chaotic billiards. In billiards where a particle moves with constant velocity and reflects off the border in accordance with the law: "the incidence angle is equal to the reflection angle". The angles and positions taken by the particle can be treated as random variables, which encouraged us to use it in the construction of a new PRNG. Sinai billiards is the first class of chaotic billiards, it is also called the dispersion system. A circular disc inside the billiard causes divergent trajectories.

This work is organized as follows. In Section 2, we present the Sinai billiard, its geometric shape, the direction of a particle travelling in the billiard table and its chaotic properties. In Section 3 we give a detailed description of our PRNG. A validation of the PRNG by test batteries and a study chaotic behavior of the sequences generated by our generator are reported in Section 4. In the final section, we draw a conclusion.

2 Presentation of the Sinai Billiard

The Sinai Billiard (Figure 1) is a planar area, consisting of a square of side $2a$ and a circular barrier with radius $r < a$ is placed at the center. A free billiard two-dimensional ($2D$) witch was proposed by Sinai in 1970 [26]. Billiards emerged to simplify the study of the behavior of two discs (gas molecule) bouncing by mutual collisions in a square. The dynamics of two interacting disks reduces to that of Sinai billiard. The billiard is sometimes called the Lorentz gas. The notations of the paper is listed in Table 1.

Table 1: Notations

$PRNG$	Pseudo-random number generator
S	the random sequence $S = S_1\, S_2\, \ldots$
Pw	Password
L	Password lenght
$[\,]$	The integer part
$\overline{p}$	Invert bits of p
A^i	The collision point at the i^{th} step
$D(O, D_n)$	The distance from O to D_n
Δ_n	Discriminant
f	Transition function
$\bigoplus$	Bitwise exclusive OR operator
HD	Hamming distance
$\|$	Concatenation operation

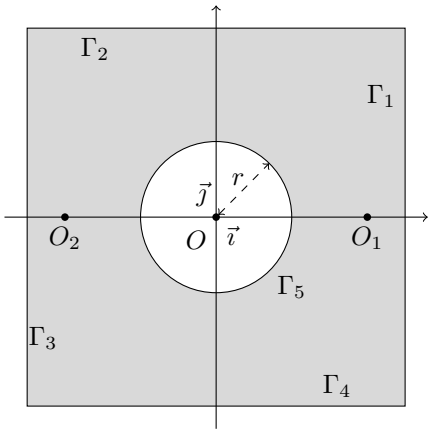

Figure 1: Sinai billard

2.1 The Billiard Geometric and Particle Direction Description

In an orthonormal $(O, \vec{\imath}, \vec{\jmath})$, we are interested in the billiard whose border $\Gamma = \cup_{i=1}^{5}\Gamma_i$ (Figure 1), is constituted by a square with side $2a$ and a circular hole of center O and raduis $r < \frac{3}{2}a$. A closed domain limited by portions in Euclidean space in two dimensions $\mathbb{R}^2$. The set $s = \cup_{i\neq j}^{4}\Gamma_i \cap \Gamma_j$ is the singular part of the border, it is composed of 4 points and $\Gamma \setminus s$ is the set of regular points of the border. In any regular point there is an internal normal vector $\overrightarrow{N}$. A point particle travels the billiard at a constant velocity v. When it reaches the border, undergoes elastic collision with specular reflection according to the law of reflection, the angle of incidence is equal to the angle of reflection with respect to $\overrightarrow{N}$ the normal vector at the border collision point. Between two collisions, the particle follows a straight path.

Initially, the particle oriented at an angle $\theta_0 = (\vec{\imath}, \overrightarrow{v_0})$ where $\vec{\imath}$ is the unit vector of x-axis. We have:

$$\overrightarrow{v_0} = \cos(\theta_0)\vec{\imath} + \sin(\theta_0)\vec{\jmath}.$$

After collision, we have Equation (1):

$$(\vec{\imath}, \overrightarrow{v_{new}}) = (\vec{\imath}, \overrightarrow{v_{old}}) + (\overrightarrow{v_{old}}, \overrightarrow{N}) + (\overrightarrow{N}, \overrightarrow{v_{new}}) \mod 2\pi. \quad (1)$$

After collision rule, we have:

$$(\overrightarrow{N}, \overrightarrow{v_{new}}) = (\overrightarrow{-v_{old}}, \overrightarrow{N}).$$

We have also:

$$(\overrightarrow{-v_{old}}, \overrightarrow{N}) = (\overrightarrow{-v_{old}}, \overrightarrow{v_{old}}) + (\overrightarrow{v_{old}}, \overrightarrow{N}) \mod 2\pi$$

$$= \pi + (\overrightarrow{v_{old}}, \overrightarrow{N}) \mod 2\pi.$$

Therefore Equation (1) becomes:

$$(\vec{\imath}, \overrightarrow{v_{new}}) = (\vec{\imath}, \overrightarrow{v_{old}}) + 2(\overrightarrow{v_{old}}, \overrightarrow{N}) + \pi \mod 2\pi. \quad (2)$$

At the $(n+1)^{th}$ collision, where $n \geq 0$, we put $\theta_n = (\vec{\imath}, \overrightarrow{v_{old}})$ and we obtain $\theta_{n+1} = (\vec{\imath}, \overrightarrow{v_{new}})$ and therefore Equation (2) becomes:

$$\theta_{n+1} = \theta_n + 2(\overrightarrow{v_n}, \overrightarrow{N_{n+1}}) + \pi \mod 2\pi \quad (3)$$

such as:

$$\overrightarrow{v_n} = \cos(\theta_n)\vec{\imath} + \sin(\theta_n)\vec{\jmath}$$

where $\overrightarrow{N_{n+1}}$ the unit normal vector at the border to the $(n+1)^{th}$ collision. We have after the geometric shape of the billiard:

$$\overrightarrow{N_{n+1}} = \begin{cases} -\dfrac{x_{n+1}}{|x_{n+1}|} & \text{if } |x_{n+1}| = a \\ -\dfrac{y_{n+1}}{|y_{n+1}|} & \text{if } |y_{n+1}| = a \\ \dfrac{x_{n+1}\vec{\imath} + y_{n+1}\vec{\jmath}}{\sqrt{x_{n+1}^2 + y_{n+1}^2}} & \text{otherwise} \end{cases}$$

We consider $A_{n+1}(x_{n+1}, y_{n+1})$ the point of $(n+1)^{th}$ collision, therefore A_{n+1} belongs to the intersection of the particles trajectory with billiard border Γ.
We define f, the transition function from (A_n, θ_n) to (A_{n+1}, θ_{n+1}) such as:

$$(x_{n+1}, y_{n+1}, \theta_{n+1}) = f(x_n, y_n, \theta_n).$$

2.2 The Transition Function f Description

We give the algorithm description of the transition function f between two collisions A_n and A_{n+1}:

$$f\colon [-a\,;a]^2 \times [0\,;2\pi[\to [-a;a]^2 \times [0\,;2\pi]$$

$$(x_n, y_n, \theta_n) \mapsto (x_{n+1}, y_{n+1}, \theta_{n+1}).$$

The equation of motion particle between two collisions is:

$$(D_n)\colon \sin(\theta_n)x - \cos(\theta_n)y - \sin(\theta_n)x_n + \cos(\theta_n)y_n = 0. \quad (4)$$

a) For $\theta_n \notin \left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}$.
From Equation (4), we have $y = \tan(\theta_n)(x - x_n) + y_n$,

we put $g_n(x) = \tan(\theta_n)(x - x_n) + y_n$ and we have $x = \cot(\theta_n)(y-y_n)+x_n$, we put $h_n(y) = \cot(\theta_n)(y-y_n)+x_n$.

The distance from O to D_n is:

$$d(O, D_n) = |-x_n \sin(\theta_n) + y_n \cos(\theta_n)|\,.$$

1) In case where $A_{n+1} \in (D_n) \cap \Gamma_5$.
$A_{n+1} \in (D_n) \cap \Gamma_5$ then $d(O, D_n) \leq r$ and $A_n \notin \Gamma_5$, therefore:

$$\begin{cases} (x_{n+1})^2 + (y_{n+1})^2 = r^2 \\ \sin(\theta_n)x_{n+1} - \cos(\theta_n)y_{n+1} - \sin(\theta_n)x_n + \cos(\theta_n)y_n = 0 \end{cases}$$

$$\Updownarrow$$

$$\begin{cases} (x_{n+1})^2 + (y_{n+1})^2 = r^2 \\ y = \tan(\theta_n)(x - x_n) + y_n = g_n(x) \end{cases}$$

We find

$$\begin{cases} (x_{n+1})^2 + (y_{n+1})^2 = r^2 \\ (5) \begin{cases} \dfrac{1}{\cos^2(\theta_n)}(x_{n+1})^2 + 2(y_n - \tan(\theta_n)x_n)\tan(\theta_n)x_{n+1} \\ +(y_n - \tan(\theta_n)^2 - r^2 = 0 \end{cases} \end{cases}$$

$\triangle_n$ discriminant of (5) is defined as:

$$\triangle_n = 4\Big(\frac{r^2}{\cos^2(\theta_n)} - (y_n - \tan(\theta_n)^2\Big)$$

Two possible solutions are:

$$x_{n+1} = \cos^2(\theta_n)\Big(- \big(y_n - \tan(\theta_n)\big)\tan(\theta_n) - \frac{\sqrt{\triangle_n}}{2}\Big)$$

or

$$x_{n+1} = \cos^2(\theta_n)\Big(- \big(y_n - \tan(\theta_n)\big)\tan(\theta_n) + \frac{\sqrt{\triangle_n}}{2}\Big)$$

and $y_{n+1} = g(x_{n+1})$. For $\theta_n \in \Big[0, \frac{\pi}{2}\Big] \cup \Big[\frac{3\pi}{2}, \pi\Big]$, we have:

$$x_{n+1} = \cos^2(\theta_n)\Big(- \big(y_n - \tan(\theta_n)\big)\tan(\theta_n) - \frac{\sqrt{\triangle_n}}{2}\Big)$$

and for $\theta_n \in \Big[\frac{\pi}{2}, \pi\Big] \cup \Big[\pi, \frac{3\pi}{2}\Big]$ we have:

$$x_{n+1} = \cos^2(\theta_n)\Big(- \big(y_n - \tan(\theta_n)\big)\tan(\theta_n) + \frac{\sqrt{\triangle_n}}{2}\Big)$$

2) In case where $A_{n+1} \in (D_n) \cap (\cup_{i=1}^4 \Gamma_i)$.
$A_{n+1} \in (D_n) \cap (\cup_{i=1}^4 \Gamma_i)$ then $d(O, D_n) > r$ or $A_n \in \Gamma_5$ for $\theta_n \in \Big[0, \frac{\pi}{2}\Big] \cup \Big[\frac{3\pi}{2}, 2\pi\Big]$, we have:

$$(x_{n+1}, y_{n+1}) = \begin{cases} \big(a, g_n(a)\big) & \text{if } -a \leq g_n(a) \leq a \\ \big(h_n(a), a\big) & \text{if } g_n(a) > a \\ \big(h_n(-a), -a\big) & \text{otherwise} \end{cases}$$

for $\theta_n \in \Big[\frac{\pi}{2}, \pi\Big] \cup \Big[\pi, \frac{3\pi}{2}\Big]$, we have:

$$(x_{n+1}, y_{n+1}) = \begin{cases} \big(-a, g_n(-a)\big) & \text{if } -a \leq g_n(-a) \leq a \\ \big(h_n(a), a\big) & \text{if } g_n(-a) > a \\ \big(h_n(-a), -a\big) & \text{otherwise} \end{cases}$$

b) For $\theta_n \in \Big\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\Big\}$.

1) In case where $\theta_n \in \Big\{\frac{\pi}{2}, \frac{3\pi}{2}\Big\}$.

$$(x_{n+1}, y_{n+1}) =$$

$$\begin{cases} (x_n, a) & \text{if } A_n \in \Gamma_5 \text{ and } y_n \geq 0 \\ (x_n, -a) & \text{if } A_n \in \Gamma_5 \text{ and } y_n < 0 \\ (x_n, \sqrt{r^2 - x_n^2}) & \text{if } A_n \notin \Gamma_5 \text{ and } -r < x_n < r \text{ and } y_n \geq 0 \\ (x_n, -\sqrt{r^2 - x_n^2}) & \text{if } A_n \notin \Gamma_5 \text{ and } -r < x_n < r \text{ and } y_n < 0 \\ (x_n, -y_n) & \text{otherwise} \end{cases}$$

2) In case where $\theta_n \in \{0, \pi\}$.

$$(x_{n+1}, y_{n+1}) =$$

$$\begin{cases} (a, y_n) & \text{if } A_n \in \Gamma_5 \text{ and } x_n \geq 0 \\ (-a, y_n) & \text{if } A_n \in \Gamma_5 \text{ and } x_n < 0 \\ (\sqrt{r^2 - y_n^2}, y_n) & \text{if } A_n \notin \Gamma_5 \text{ and } -r < y_n < r \text{ and } x_n \geq 0 \\ (-\sqrt{r^2 - y_n^2}, y_n) & \text{if } A_n \notin \Gamma_5 \text{ and } -r < y_n < r \text{ and } x_n < 0 \\ (-x_n, y_n) & \text{otherwise} \end{cases}$$

2.3 The Sinai Billiards Chaotic and Ergodic Properties

After the publication of the Article [26] in 1970, Sinai billiard has become popular, it has undergone many subsequent studies by many mathematicians and physicists authors [3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 26, 27]. The system shows a completely chaotic behavior [12, 26].

In general, the geometric shape of its boundaries determines dynamic billiards properties. It may consist of a convex curve, concave or linear. Sinai has shown in [26] that all billiards with the outwardly convex borders are always strongly chaotic. In [12], Per Dahlqvist has calculated an explicit expression of the Lyapunov exponent λ of Sinai billiard. λ measure quantitatively the chaos of dynamical systems, being positive means that there is a dependence on initial conditions (i.e the chaos existence). λ is positive for all values of the radius r of the disc.

Sinai has developed a method to prove that all dispersing billiard (Sinai billiard) is ergodic, mixing and it has a stronger property, the K-mixing. Moreover Gallavotti and Ornstein proved in [14] that the Sinai billiard is a Bernoulli system. The Bernoulli property is the strongest among the ergodic properties. It involves K-mixing, mixing and ergodicity.

3 Designing a PRNG Based on the Sinai Billiard

It is a deterministic pseudo-random numbers generator initialized by a password the Pw with arbitrary sized, the output is a cryptographically secure binary sequence. we consider two point particles that move in the Sinai billiard with a constant velocity $\|\overrightarrow{v_1}\| = \|\overrightarrow{v_2}\| = 1$, without interaction between it. The departure point for the first particle (resp. second particle) is O_1 (resp. O_2) such as $\overrightarrow{OO_1} = \frac{3a}{4}\vec{\imath}$ (resp. $\overrightarrow{OO_2} = -\frac{3a}{4}\vec{\imath}$). Initially, it is oriented by $\overrightarrow{v_{0,1}}$ (resp. $\overrightarrow{v_{0,2}}$) such as $\theta_{0,1} = (\vec{\imath}, \overrightarrow{v_{0,1}})$ (resp. $\theta_{0,2} = (\vec{\imath}, \overrightarrow{v_{0,2}})$) where:

$$0 \leq \theta_{0,1}, \theta_{0,2} < 2\pi.$$

The angles $\theta_{0,1}$ and $\theta_{0,2}$ are calculated from the Pw using a technique based on a pointer, it positions on the Pw bits. The pointer moves from a position to other according to a linear congruential throughout the ASCII representation of Pw.

After initialization, we performed a predetermined number of collisions for the two particles, then start generating individuals necessary for the construction of the final sequence $S = S_1\, S_2 \ldots S_i \ldots$ with $S_i = I_{i,1} \bigoplus I_{i,2}$, $I_{i,1}$ and $I_{i,2}$ are two individuals generated in the i^{th} step. At each step i two individuals $I_{i,1}$ and $I_{i,2}$ of 32 bits will be generated based on the coordinates of the collision point of two balls with the square border of the billiard.

3.1 The Initial Values $\theta_{0,1}$ and $\theta_{0,2}$ Calculation

From a password $Pw = (p_{L-1} \ldots p_2 p_1 p_0)_2$, a binary string of any length L, we calculate the initialization angles $\theta_{0,1}$ and $\theta_{0,2}$. For each angle, we need to extract 64 bits from Pw. We consider a pointer pt that takes values indicating the bit positions in the Pw. The positions suite is defined as following:

$$\begin{cases} pt(0) & = 1 \\ pt(i+1) & = \left(\left(\left[\frac{L}{2}\right] + 1\right) \times pt(i) + 1\right) \bmod (L) \text{for } i \geq 0 \end{cases}$$

The pointer moves on the Pw, every time it positions on a new bit p_i and reads the information 0 or 1 necessary to calculate $\theta_{0,1}$ and $\theta_{0,2}$. We find $I_{0,1}$ and $I_{0,2}$ ($0 \leq I_{0,1}, I_{0,2} < 2^{64}$) as following:

$$\begin{aligned} I_{0,1} &= (\overline{p}_{pt(63)}\, p_{pt(62)} \cdots p_{pt(2)}\, \overline{p}_{pt(1)}\, p_1)_2 \\ &= p_1 + \sum_{i=0}^{31} \overline{p}_{pt(2\times i+1)} \times 2^i + \sum_{i=1}^{31} p_{pt(2\times i)} \times 2^i \end{aligned}$$

and

$$\begin{aligned} I_{0,2} &= (p_{L-1-pt(63)}\, \overline{p}_{L-1-pt(62)} \cdots p_{L-1-pt(1)}\, \overline{p}_{L-2})_2 \\ &= \overline{p}_{L-2} + \sum_{i=0}^{31} p_{pt(2\times i+1)} \times 2^i + \sum_{i=1}^{31} \overline{p}_{pt(2\times i)} \times 2^i \end{aligned}$$

finally

$$\theta_{0,1} = \frac{2\pi \times I_{0,1}}{2^{64}} \quad \text{and} \quad \theta_{0,2} = \frac{2\pi \times I_{0,2}}{2^{64}}$$

We call Initialize the initial values $\theta_{0,1}$ and $\theta_{0,2}$ calculation algorithm (Algorithm 1).

Algorithm 1 Calculation of $\theta_{0,1}$ and $\theta_{0,2}$

1: Begin
2: On taking password $Pw = (p_{L-1} \ldots p_2 p_1 p_0)_2$ a binary string of any length L .
3: $pt \leftarrow 1$
4: $I_{0,1} \leftarrow p_1$
5: $I_{0,2} \leftarrow p_{L-2}$
6: **for** $i = 1$ to 63 **do**
7: $\quad pt \leftarrow \left(\left(\left[\frac{L}{2}\right] + 1\right) \times pt + 1\right) \bmod (L)$
8: $\quad$ **if** i is even **then**
9: $\quad\quad I_{0,1} \leftarrow I_{0,1} + \overline{p}_{pt} \times 2^i$
10: $\quad\quad I_{0,2} \leftarrow I_{0,2} + p_{L-1-pt} \times 2^i$
11: $\quad$ **else** {i is odd}
12: $\quad\quad I_{0,1} \leftarrow I_{0,1} + p_{pt} \times 2^i$
13: $\quad\quad I_{0,2} \leftarrow I_{0,2} + \overline{p}_{L-1-pt} \times 2^i$
14: $\quad$ **end if**
15: **end for**
16: $\theta_{0,1} \leftarrow \frac{2\pi \times I_{0,1}}{2^{64}}$
17: $\theta_{0,2} \leftarrow \frac{2\pi \times I_{0,2}}{2^{64}}$
18: End

3.2 Generating the Pseudo-random Sequence

After calculating the initialization's angles $\theta_{0,1}$ and $\theta_{0,2}$, the two particles are ready to travel the billiard. Before starting to generate the individuals, we let the particles circulate and hit the billiard's wall until the e^{th} collision, we get $(x_k^0, y_k^0, \theta_k^0) = f^e(x_{0,k}, y_{0,k}, \theta_{0,k})$ for $k = 1, 2$ where e ($0 \leq e \leq 255$) is determined from the last 8 bits of the password $Pw = (p_{L-1} \ldots p_2 p_1 p_0)_2$ such as:

$$e = \sum_{i=0}^{7} p_i \times 2^i$$

At every step $i (i \geq 1)$, we carry out $(n_i + 1)$ collisions for both particles with $n_i (0 \leq n_i \leq 3)$ is determined by 2 bits taken directly from the password Pw as follows:

$$n_i = 2 \times p_{j+1} + p_j$$

where

$$j = 2 \times i \bmod (L - 1).$$

After $(n_i + 1)$ collisions, New coordinates are obtained $(x_k^i, y_k^i, \theta_k^i) = f^{n_i+1}(x_k^{i-1}, y_k^{i-1}, \theta_k^{i-1})$. We are interested in the collision coordinates with the square border of the billiard (i.e $|x_k^i| = a$ and $|y_k^i| = a$) ignoring the collisions

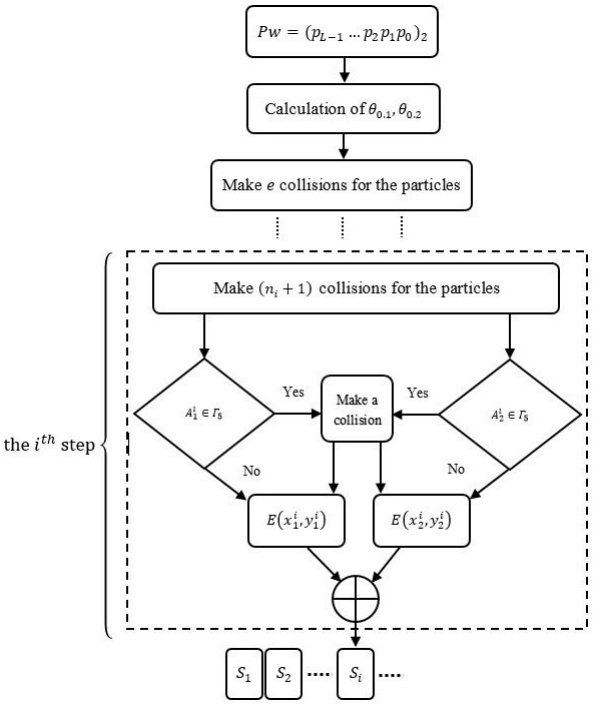

Figure 2: an operation step of our PRNG

with circle. If $A_k^i \in \Gamma_5$ (i.e $(x_k^i)^2 + (y_k^i)^2 = r^2$), we go to the next collision point for k^{th} particle $(x_k^i, y_k^i, {}^i_k) \longleftarrow f^{n_i+2}(x_k^{i-1}, y_k^{i-1}, \theta_k^{i-1})$, and then two individuals are generated values:

$$E(x_k^i, y_k^i) = \begin{cases} \left[2^{32}\frac{x_k^i}{a}\right] & \text{if } x_k^i \geq 0 \text{ and } \left|y_k^i\right| = a \\ \left[2^{32}\left(1 + \frac{x_k^i}{a}\right)\right] & \text{if } x_k^i < 0 \text{ and } \left|y_k^i\right| = a \\ \left[2^{32}\frac{y_k^i}{a}\right] & \text{if } y_k^i \geq 0 \text{ and } \left|x_k^i\right| = a \\ \left[2^{32}\left(1 + \frac{y_k^i}{a}\right)\right] & \text{if } y_k^i < 0 \text{ and } \left|x_k^i\right| = a \end{cases}$$

$$= I_{i,k} = (b_{31}^{i,k} b_{30}^{i,k} \dots b_1^{i,k} b_0^{i,k})_2$$

The output S of the PRNG is the concatenation of the sub-sequences $S_1, S_2, \dots, S_i \dots$ then:

$$S = S_1 S_2 \dots S_i \dots,$$

with

$$S_i = I_{i,1} \bigoplus I_{i,2},$$

where $I_{i,1}$ and $I_{i,2}$ two individuals are generated at the i^{th} step.

The algorithm have two input parameters, a password Pw and an integer N which indicates the length of the requested binary sequence as shown in (Algorithm 2).

Algorithm 2 Generation the random suit RS

```
Begin
θ1, θ2 ← Initialize(Pw)
(x1, y1) ← (0, 3/2 a)
(x2, y2) ← (0, −3/2 a)
e ← p0
for i = 1 to 7 do
    e ← e + p_i × 2^i
end for
(x1, y1, θ1) ← f^e(x1, y1, θ1)
(x2, y2, θ2) ← f^e(x2, y2, θ2)
I_{0,1} ← p1
I_{0,2} ← p_{L−2}
i ← 1
j ← i mod (L − 1)
n ← 2 × p_{j+1} + p_j
l ← 0
while l < ⌈N/32⌉ do
    (x1, y1, θ1) ← f^{n+1}(x1, y1, θ1)
    (x2, y2, θ2) ← f^{n+1}(x2, y2, θ2)
    if (x1)^2 + (y1)^2 = r^2 then
        (x1, y1, θ1) ← f(x1, y1, θ1)
    end if
    if (x2)^2 + (y2)^2 = r^2 then
        (x2, y2, θ2) ← f(x2, y2, θ2)
    end if
    I1 ← E(x1, y1)
    I2 ← E(x2, y2)
    RS ← RS||(I1 ⊕ I2)
    l ← l + 1
    i ← i + 1
    j ← 2 × i mod (L − 1)
end while
End
```

4 Security Analysis

A PRNG should verify security properties to resist the attacks. The security analysis must be done with care to assess the quality of the sequences. We study in the following paragraphs, the key space size, sensitivity to initial conditions and the level of randomness of the sequences. In the following study we fixed r at $\frac{a}{2}$.

4.1 The Key Space

The size of the key space is among the criteria by which a crypto-systems to be robust, a large size makes brute force attacks infeasible. Our algorithm has as an initialization key, a binary string of any size as mentioned above. The two particles billiards need exactly 128 bits to calculate its initial orientations. These 128 bits are extracted via a pointer that traverses the password Pw. This leads us to say that the size of the key space is large enough to be attacked exhaustively.

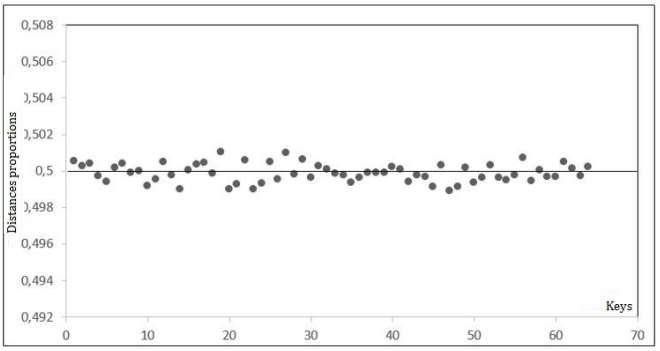

Figure 3: The proportion $\frac{DH(S^0, S^i)}{N}$

4.2 Sensitivity to Key

The sensitivity to a small change in the key is one of the essential properties for a PRNG. In other words, a small difference in the seeds of the system should cause a big change in the pseudo-random sequences. This property makes the generator highly secured against statistics and differential attacks, and so the sequence can not be broken even if there is a small difference between the keys. In our case, the generator is based on two dynamic systems of a purely chaotic billiard [12, 26]. In fact, to analyze the chaotic behavior of our generator, we place several k_i keys in the input of the generator with a bit of difference between it. A pseudo-random sequences S^i of size $N = 10^6$ are generated. The Hamming distance between two binary sequences $S^i = x_{1,i}\, x_{2,i} \ldots x_{N,i}$ and $S^j = x_{1,j}\, x_{2,j} \ldots x_{N,j}$ of equal length N is the number $DH(S^i, S^j) = card\{d/\, x_{d,i} \neq x_{d,j}\}$. Thus, for the two binary sequences S_i and S_j, the Hamming distance is given by:

$$DH(S^i, S^j) = \sum_{t=1}^{N} x_{t,i} \bigoplus y_{t,i}$$

In the case where the generator is chaotic, this distance is generally ranges around $\frac{N}{2}$, witch gives $\frac{DH(S^i, S^j)}{N}$ is approximately 0.5 for each pair of sequences produced.

We generate a group of pseudo-random sequences $\{S^i\}_{0 \leq i \leq 64}$ using the keys $\{k_i\}_{0 \leq i \leq 64}$. the key k_0 = "$GUENNOUN$", its binary representation in ASCII code is k_0 = (01000111 01000101 010011100100111 01001111 01010101 01001110)$_2$. The other 64 keys $\{k_i\}_{1 \leq i \leq 64}$ are derived from k_0, by changing the i^{th} bit among the 64 bits of k_0 to find k_i. The value $\frac{DH(S^0, S^i)}{N}$ between the sequences is shown in the graph 3.

From the results obtained, the differences in proportions between the sequences are approximately 0.5, indicating that the proposed generator is highly sensitive to initial conditions. Sensitivity to a small perturbation in the key for our generator is due to two reasons:

1) The generator is based in its construction on a system of a chaotic billiard, so the generated sequences inherit the chaos and unpredictability of the billiard. A number additional of iterations extracted directly from the password allows the generator to benefit maximally of the chaos offered by the billiard;

2) The initialization angles are taken from the Pw, using a pointer that points to different positions until the its total cover. Indeed, a difference in a bit between two keys may cause a different orientation to the particles and thus to the generated sequences.

Sinai billiard is chaotic for all values of the radius r, but there is a difference in the chaos level for each value of r as shown in [12] where the Lyapunov exponent is expressed in terms of r. Therefore, the user can control the level of the chaos generator by an input parameter at the algorithm (r, where $0 < r < \frac{3}{2}a$).

In the next section, we examine the randomness of the generator by statistical tests NIST (National Institute of Standards and Technology), which are considered the most valued.

4.3 Statistical Tests

The NIST Statistical Test Suite [24] is a statistical package, the result of collaboration between the statistical Engineering Division (SED) at NIST and the Computer Security Division. This suite consists of 16 tests, developed to quantify and assess the degree of random binary sequences produced by cryptographic generators. For each statistical test, a P_{value} is calculated from the bit sequence. This P_{value} is compared to a predefined threshold α, which is also called significance level. If P_{value} is greater than α, then the sequence is considered to be random with $1 - \alpha$ confidence level, and it proceeds the statistical test successfully, otherwise the sequence does not appear random. Generally, as suggested by NIST, α is set to its default value of 0.01, it indicates that one would expect 1 sequence in 100 sequences to be rejected.

To test our PRNG and as recommended by the NIST, we generated 1000 sequences, the length of each sequence is 1000^6 from a randomly selected keys. The test results on the sequences are presented in Table 2.

The minimum pass rate for the test Random Excursions (Variant) is approximately 609 for a sample of 625 binary sequences. The minimum pass rate for other tests is approximately 980 for a sample of 1000 binary sequences. We can see that the number of sequences that have managed to pass each test is greater than the minimum rate. Therefore, the proposed generator passed all NIST statistical tests. We can conclude that the numbers generated by the PRNG are random.

Table 2: Results of testing our generator on NIST test suite

Test Name	The P_{value}	The proportion	Result
Frequency	0.695200	992/1000	Success
Block-Frequency	0.861264	990/1000	Success
Cumulative Sums (1)	0.169981	995/1000	Success
Cumulative Sums (2)	0.978072	991/1000	Success
Runs	0.542228	985/1000	Success
Longest Run	0.709558	985/1000	Success
Rank	0.169981	995/1000	Success
FFT	0.080027	984/1000	Success
Non-Overlapping	0.505854	987/1000	Success
Overlapping	0.041169	991/1000	Success
Universal	0.334538	991/1000	Success
Approximate Entropy	0.851383	989/1000	Success
Random Excursions	0.478175	616/625	Success
Random Excursions Variant	0.470796	616/625	Success
Serial (1)	0.919131	986/1000	Success
Serial (2)	0.334538	980/1000	Success
Linear Complexity	0.948298	992/1000	Success

5 Conclusion

The PRNG proposed after a rigorous analysis, showed encouraging results, it is sensitive to a small change in the key and passed the NIST statistical test suite. Our generator has inherited the Sinai billiard unpredictability. It can be used for critical cryptographic applications. Furthermore, the systems of the chaotic billiards are good candidates to get into new cryptographic system design.

References

[1] M. Ahmad, B. Alam, and O. Farooq, "Chaos based mixed keystream generation for voice data encryption," *arXiv preprint arXiv: 1403.4782*, 2014.

[2] M. Andrecut, "Logistic map as a random number generator," *International Journal of Modern Physics B*, vol. 12, no. 9, pp. 921–930, 1998.

[3] M. V. Berry, "Quantizing a classically ergodic system: Sinai's billiard and the KKR method," *Annals of Physics*, vol. 131, no. 1, pp. 163–216, 1981.

[4] L. A. Bunimovich, "On billiards close to dispersing," *Matematicheskii Sbornik*, vol. 136, no. 1, pp. 49–73, 1974.

[5] L. A. Bunimovich, "On ergodic properties of certain billiards," *Functional Analysis and Its Applications*, vol. 8, no. 3, pp. 254–255, 1974.

[6] L. A. Bunimovich, Y. G. Sinai, and N. I. Chernov, "Statistical properties of two-dimensional hyperbolic billiards," *Russian Mathematical Surveys*, vol. 46, no. 4, pp. 47–106, 1991.

[7] N. Chernov and R. Markarian, "Chaotic billiards," *Mathematical Surveys and Monographs*, vol. 127, 2006.

[8] N. I. Chernov, "Sinai billiards under small external forces," *Annales Henri Poincaré*, vol. 2, pp. 197–236, Springer, 2001.

[9] N. I. Chernov and C. Haskell, "Nonuniformly hyperbolic k-systems are bernoulli," *Ergodic Theory and Dynamical Systems*, vol. 16, no. 1, pp. 19–44, 1996.

[10] N. Chernov, "Decay of correlations and dispersing billiards," *Journal of Statistical Physics*, vol. 94, no. 3-4, pp. 513–556, 1999.

[11] N. Chernov and L. S. Young, "Decay of correlations for lorentz gases and hard balls," *Hard Ball Systems and the Lorentz Gas*, pp. 89–120, Springer, 2000.

[12] P. Dahlqvist, "The lyapunov exponent in the sinai billiard in the small scatterer limit," *Nonlinearity*, vol. 10, no. 1, pp. 159, 1997.

[13] P. Dahlqvist and R. Artuso, "On the decay of correlations in sinai billiards with infinite horizon," *Physics Letters A*, vol. 219, no. 3, pp. 212–216, 1996.

[14] G. Gallavotti and D. S. Ornstein, "Billiards and bernoulli schemes," *Communications in Mathematical Physics*, vol. 38, no. 2, pp. 83–101, 1974.

[15] C. Guyeux, Q. Wang, and J. M. Bahi, "A pseudo random numbers generator based on chaotic iterations: Application to watermarking," in *Web Information Systems and Mining*, pp. 202–211, Springer, 2010.

[16] A. Jolfaei and A. Mirghadri, "Image encryption using chaos and block cipher," *Computer and Information Science*, vol. 4, no. 1, pp. 172, 2010.

[17] L. Kocarev, G. Jakimoski, T. Stojanovski, and U. Parlitz, "From chaotic maps to encryption schemes," in *Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS'98)*, vol. 4, pp. 514–517, 1998.

[18] A. Lasota and M. C. Mackey, *Chaos, Fractals, and Noise: Stochastic Aspects of Dynamics*, vol. 97, Springer Science & Business Media, 1998.

[19] S. Li, Q. Li, W. Li, X. Mou, and Y. Cai, "Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding," in *Cryptography and Coding*, pp. 205–221, Springer, 2001.

[20] S. Lian, J. Sun, J. Wang, and Z. Wang, "A chaotic stream cipher and the usage in video protection," *Chaos, Solitons & Fractals*, vol. 34, no. 3, pp. 851–859, 2007.

[21] S. Oishi and H. Inoue, "Pseudo-random number generators and chaos," *IEICE Transactions*, vol. 65, no. 9, pp. 534–541, 1982.

[22] V. Patidar and K. K. Sud, "A novel pseudo random bit generator based on chaotic standard map and its testing," *Electronic Journal of Theoretical Physics*, vol. 6, no. 20, pp. 327–344, 2009.

[23] V. Patidar, K. K. Sud, and N. K. Pareek, "A pseudo random bit generator based on chaotic logistic map and its statistical testing," *Informatica*, vol. 33, no. 4, 2009.

[24] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, Technical Report, DTIC Document, 2001.

[25] F. Shang, K. Sun, and Y. Cai, "An efficient mpeg video encryption scheme based on chaotic cipher," in *IEEE Congress on Image and Signal Processing (CISP'08)*, vol. 3, pp. 12–16, 2008.

[26] Y. G. Sinai, "Dynamical systems with elastic reflections," *Russian Mathematical Surveys*, vol. 25, no. 2, pp. 137–189, 1970.

[27] L. S. Young, "Statistical properties of dynamical systems with some hyperbolicity," *Annals of Mathematics*, vol. 147, no. 3, pp. 585–650, 1998.

[28] F. Zheng, X. J. Tian, J. Y. Song, and X. Y. Li, "Pseudo-random sequence generator based on the generalized henon map," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, no. 3, pp. 64–68, 2008.

Khalid Charif is a Ph.D student at the Faculty of Science, Mohamed V University in Rabat. He obtained his master's degree in mathematics and statistics, option cryptography and information security at the same university in 2013. His research interests include information security and cryptography.

Ahmed Drissi received his Ph.D degree in cryptology from the Faculty of Science, University Ibn Zohr Agadir, Morocco in 2014. His research interests include Code theory and the Cryptology. Currently he is associate member of the Laboratory for Analysis, Algebra and decision aid (LA3D). Faculty of Sciences Rabat, Morocco.

Zine El Abidine Guennoun is a professor of Department of Mathematics at the Faculty of Science, Mohamed V University in Rabat, Morocco. He received his Ph.D. (1989). His research interests include non linear analysis, fixed point theory, differential equation, financial mathematics and cryptography.