Applied Mathematics, 2012, 3, 1664-1673
http://dx.doi.org/10.4236/am.2012.311230 Published Online November 2012 (http://www.SciRP.org/journal/am)

A Novel Pseudo Random Number Generator Based on Two Plasmonic Maps

Michael François[1], Thomas Grosges[1], Dominique Barchiesi[1], Robert Erra[2]
[1]Group for Automatic Mesh Generation and Advanced Methods, Gamma 3 Project (UTT-INRIA), University of Technology of Troyes, Troyes Cedex, France
[2]Network & Information Security, Graduate School of Informatic, Electronic, Automatic (ESIEA), Paris, France
Email: thomas.grosges@utt.fr

Received August 29, 2012; revised September 29, 2012; accepted October 7, 2012

ABSTRACT

In plasmonic systems, the response of nanoobjects under light illumination can produce complex optical maps. Such plasmonic or resonant systems have interesting characteristics such as sensitivity on parameters and initial conditions. In this paper, we show how these complex maps can be cryptographically improved and associated in order to design a secure pseudo random number generator.

Keywords: Plasmonics; Applied Classical Electromagnetism; Pseudo-Random Number Generator; Randomness; Cryptography; Remeshing Process

1. Introduction

Pseudo-random number generators (PRNGs) are fundamental blocks in various domains of applications such as Monte Carlo simulation algorithms, communications and many cryptographic systems which depend on the quality of the pseudo random sequences. The generated numbers are mainly used as simple pseudo random sequences, private or secret keys or secret signatures. The development of PRNGs has impassioned the researchers for few decades and since then, many techniques to produce such PRNGs have been studied [1-9]. The robustness of such pseudo random generators is crucial to ensure secure applications in cryptograhy and to avoid all the various and existing attacks. A large family of PRNGs is based on sequences generated by single chaotic system or combination of chaotic maps [4,8,10,11], through a one-way function. Such a combination of several maps by a one-way function improves the security of the PRNG. In this paper, we propose a PRNG based on the use of complex maps produced by the electromagnetic response of plasmonic systems. The study of plasmonic or resonant systems has shown the possibility to produce complex electromagnetic field patterns, with strong gradients and high confinement, superimposed with interference patterns. These local physic effects have opened the experimental and theoretical ways of designing efficient systems in various new applications (sensors, imaging and burning biomedicine applications, security) [12-15]. For cryptographic applications, the main question concerns the ability of such plasmonic systems, due to their high sensitivities to parameters in the neighbouring of the resonances, to serve as the basis of pseudo random number generator with high efficiency.

Therefore, we propose a method to generate long sequences of numbers, with high quality of randomness, based on the complex nature of plasmon simulations. The nanosystems permit to produce complex optical maps and provide inherent tamper-evidence due to their sensitivities to the initial parameters and initial conditions. We show how these complex maps, through a numerical process, can produce sequences that have high level of randomness, in compliance with the classical tests of randomness on binary sequences [16]. This can be used as a base of secret key between two parties in a symmetric cipher (e.g. One-time pad). The high level of security of this inspired-plasmonic system is related to the number of freedom degrees used to generate the pseudo random sequence and the physical complexity of the plasmonic structures. These degrees of freedom can be grouped into two categories of parameters, of completely different origin. The first one ($\mathcal{K}_P$) can be related to the physical parameters required to model the nanostructures (materials, shapes). From the constructed 3D spatial maps of the electromagnetic field, a second set of parameters ($\mathcal{K}_N$) can be assigned to a numerical processes consisting in an adaptive remeshing process and a modular transformation. These processes ensure quality targets of a maximum Shannon's entropy [17] as well as increasing disorder in the sequences. We analyse the randomness quality [16] and the correlation of sets of pseudo random sequences. We show that only weak correlation can be exhibited. This weak correlation between pseudo random sequences is an essential condition to be fulfilled for more secure uses.

This paper is structured as follows. The description of the method as well as the plasmonic functions analysis are given in Section 2. Section 3 presents results for constructed pseudo random sequences and statistical analysis applied on the sets of generated pseudo random sequences. The security analysis of the PRNG is also discussed, before concluding in Section 4.

2. The Proposed Cryptosystem

The core of the PRNG algorithm is based on the contruction of two plasmonic maps obtained by computing the electromagnetic field interacting with metallic nanoparticles.

2.1. Nanoworld as Source of Complex Maps

The process of production of pseudo random sequences we propose, is based on a model of plasmonic resonance [14,18]. The interest here is the interaction of the coupling of light-matter at a nanometric scale which is kwown to induce strong gradient of the field and complex interference patterns. The resonance of the interaction between light and matter is very sensitive to all physical parameters: size of the nanoobjects, materials and illumination characteristics. The numerical simulated signals on which we work is the total electromagnetic field in the vicinity of such metallic nanostructures. It comes from the numerical resolution of the vectorial Helmholtz' equation governing the electric field vector and the Maxwell's equations relating both electric and magnetic field vectors $\boldsymbol{E}$ and $\boldsymbol{H}$ satisfying:

$$\nabla\times\left(\frac{1}{\mu_r}\nabla\times\boldsymbol{E}\right)-k_0^2\varepsilon_r\boldsymbol{E}=0 \qquad (1)$$

$$\boldsymbol{H}=\frac{-j}{k_0\mu_r}\nabla\times\boldsymbol{E} \qquad (2)$$

with $k_0 = 2\pi/\lambda$, λ the wavelength in vacuum, ε_r and μ_r, the relative permittivities and permeabilities, respectively. The electric and magnetic fields $\boldsymbol{E}$ and $\boldsymbol{H}$ satisfy the orthogonality condition $\langle\boldsymbol{H}|\boldsymbol{E}\rangle=0$. The resolution of such a system of equations can be achieved numerically in a 3D spatial domain Ω and the physical electromagnetic fields $\boldsymbol{E}(x,y,z)$, $\boldsymbol{H}(x,y,z)$ and their associated intensities

$I_E(x,y,z)=\langle\boldsymbol{E}(x,y,z)|\boldsymbol{E}(x,y,z)\rangle$ and $I_H(x,y,z)=\langle\boldsymbol{H}(x,y,z)|\boldsymbol{H}(x,y,z)\rangle$ are computed. The characteristics of the 3D spatial maps are intrinsically dependent on a large number of parameters which relates to the entire physical system. It is moreover why, the exact reproducibility of this map is almost impossible for an attacker without additional information about the used physical and meshing parameters $\mathcal{K}_P$ and $\mathcal{K}_N$. The physical parameters can be grouped as a key set $\mathcal{K}_P$ containing:

1) Optical parameters: the wavelength of the light source $\lambda = 2\pi/k_0$ in $\mathbb{R}$, the incident angle of illumination θ_i in $\mathbb{R}$, the choice of material permitivitties $\varepsilon_p(\lambda)$ in $\mathbb{C}$ and ε_m in $\mathbb{C}$ for the surrounding medium;

2) Geometrical parameters: the radii of the nanospheres $\{r_p$ in $\mathbb{R}\}$, the number of nano-sphere N_p in $\mathbb{N}$ and their spatial coordinates $\{(x_i,y_i,z_i),1\le i\le N_p\}$, in $\mathbb{R}^3$.

The theoretical dimension of the space of the physical parameters $\mathcal{K}_P$ is $\mathbb{N}\times\mathbb{R}^{2+4N_p}\times\mathbb{C}^{1+N_p}$. At this stage, the complex spatial fields $\boldsymbol{E}(x,y,z)$, $\boldsymbol{H}(x,y,z)$ and their associated intensities $I_E(x,y,z)$ and $I_H(x,y,z)$ necessitate a specific numerical process in order to transform these maps to an efficient pseudo random sequence $\Psi_{\text{out}}(n)$. The aim is to obtain a sequence $\Psi_{\text{out}}(n)$ with a high level of randomness and which satisfy the basic cryptographic properties.

2.2. Construction of the Generator

The "physical" 3D maps $\boldsymbol{E}(x,y,z)$, $\boldsymbol{H}(x,y,z)$, $I_E(x,y,z)$ and $I_H(x,y,z)$ cannot be directly used as pseudo random sequences or secret keys in an encryption scheme, because the distribution of the spatial intensities is not random enough relatively to the requirements of a random sequence. Therefore a renumbering of the spatial nodes is necessary to be able to create more disorder in these intensity maps, which will give us a stronger derived sequence $\Psi_{\text{out}}(n)$. A two-steps numerical process is achieved on the field and intensity maps in order to satisfy both criterion of maximum entropy and randomness statistical characteristics.

The first step consists in an homogenization of occurrence of fields and intensities through the redistribution of intensity level by a 3D adaptive meshing process [19] with an a posteriori error estimator based on the maximum entropy. This adaptive scheme of remeshing of the domain (x,y,z) uses selected frequencies of each intensity levels occurrence as target. For this goal, second order polynomials are used to interpolate intensity levels, to generate additional points in the tomography map (or equally to suppress the nodes corresponding to too numerous intensity levels). Each point of the domain (x,y,z) is labeled by an integer n (the node number) and the intensity levels of the maps $I_E(x,y,z)$, $I_H(x,y,z)$ are translated to $I_E(n)$, $I_H(n)$ before transformed into the maps $X_E(n)$, $X_H(n)$ in the basis C. In this new basis C, the maps are given by:

$$\begin{aligned} X_E(n) = \mathcal{F}(\boldsymbol{E}(n)) &= \text{Int}\left[\alpha\left|\boldsymbol{E}(n)\right|^2\right]\text{mod } C \\ &= \text{Int}\left[\alpha\left|I_E(n)\right|\right]\text{mod } C, \end{aligned} \tag{3}$$

$$\begin{aligned} X_H(n) = \mathcal{F}(\boldsymbol{H}(n)) &= \text{Int}\left[\alpha\left|\boldsymbol{H}(n)\right|^2\right]\text{mod } C \\ &= \text{Int}\left[\alpha\left|I_H(n)\right|\right]\text{mod } C, \end{aligned} \tag{4}$$

with α and C fixed integers (e.g. $\alpha = 10^7$ and $C = 256$). This transformation of the maps $I_E(n)$ to $X_E(n)$ (resp. $I_H(n)$ to $X_H(n)$) drastically affects the internal structure of the sequence. These two maps $X_E(n)$ and $X_H(n)$ produce directly random-like images (*i.e.* images that seem to be random in appearence but not necessarely satisfying cryptographical randomness requirements). That comes from the physics structure of the fields $\boldsymbol{E}$ and $\boldsymbol{H}$ and the remeshing process which were not intended to randomize the initial maps by only to control the occurencies of the intensity levels in respect to the entropy criteria. This part of the space of parameters consists in a set of numerical parameters $\mathcal{K}_N$ associated to the remeshing process and are summary by:

the adaptive remeshing process parameters $h_{\min}$, $h_{\max}$, δ_ϕ in $\mathbb{R}\times\mathbb{R}\times\mathbb{R}$, the minimum, the maximum distance between nodes after remeshing and the maximum tolerance between the levels of signal at two adjacent nodes, respectively. The number of nodes after computation is N_n in $\mathbb{N}$ and their spatial coordinates $\left\{(x_j, y_j, z_j), 1 \le j \le N_n\right\}$, in $\mathbb{R}^3$.

With such numerical parameters, the dimension of the space $\mathcal{K}_N$ is $\mathbb{R}^3$.

The second step consists in applying a xor operator by matching $X_E(n)$ and $X_H(n)$ in order to produce a new map $\Psi_{\text{out}}(n)$. This matching benefits from the differences between $I_E(n)$ and $I_H(n)$ (*i.e.* $I_E(n)$ exhibits strong variations whenever $I_H(n)$ is smother) and coming from the orthogonality between the symmetric and antisymmetric parts of the electromagnetic tensor, respectively. This map is given by:

$$\Psi_{\text{out}}(n) = X_E(n) \oplus X_H(n), \tag{5}$$

Such a produced numerical pseudo random sequence $\Psi_{\text{out}}(n)$ is therefore deduced from the plasmonic process. The complexity of the plasmonic simulated optical signal of nano-objects and the various parameters used are the assets of this cryptosystem and the global set of parameters $\mathcal{M} = \mathcal{K}_P \cup \mathcal{K}_N$ of dimension $\mathbb{N}\times\mathbb{R}^{5+4N_p}\times\mathbb{C}^{1+N_p}$.

In principle the physical parameters used seem to take an infinity of values (*i.e.* $\mathbb{N}$, $\mathbb{R}$ or $\mathbb{R}$, even non existing materials can be used in the model). With all this parameters package, the exact reproducibility of the sequence $\Psi_{\text{out}}(n)$ is almost impossible if the exact parameters used are unknown. Indeed, in the vicinity of the plasmon resonance, an error on one of the used parameters can produce enough variations in the produced image map (in term of the exact value of the pixels in the formed image). Due to the high internal complexity and without a robust reverse engineering method, this construction process is now a good candidate for a PRNG permitting to produce a long pseudo random sequence.

A fundamental advantage of any kind of PRNG is the quality of pseudo random sequences. According to the Kerckhoffs' principle [20], the security of a cryptosystem only depends on its keys. In any cryptosystem, a poor key or a limited key space $\mathcal{K}$ induces a weakness of the cryptosystem (*i.e.* which can be easily broken by testing all possibilities: brute-force attacks). Indeed, the limit of brute-force attacks on the parameter space depends on the entropy of this space. For a given today's computer speed-up, it is commonly admise that a key space (space of parameters) of size $\mathcal{K} < 2^{128} \approx 10^{38}$ (*i.e.* smaller than 128 bits) is not sufficiently secure [21]. In the present case, the generated key space $\mathcal{M}$ permits to overpass the lower limit of 128 bits of entropy. Each key is corresponding to two kinds of input data related to numerical or physical characteristics.

3. Results and Discussion

In this section, the results on the produced pseudo random sequences are presented. Moreover, the analysis methods based on the randomness and correlation properties are discussed and applied to the generated sequences.

3.1. Generation of a Subspace of Pseudo Random Sequences

A subspace of pseudo random sequences is produced before analysing. These sequences are obtained from the simulation of a plasmonic device and the numerical remeshing process in the construction of the pseudo random sequence $\Psi_{\text{out}}(n)$. This analysis puts forward the quality of the outputs produced following a change of consecutive parameters. We consider the electromagnetic images of the interaction of light with gold nano-particles of radius r_p in [5.0; 210.0] nm embeded in a surrounding medium of permittivity ε_m in [0.999; 2.500] under light illumination wavelength λ in [480; 1200] nm and incident angle θ_i in $[0; 2\pi]$. The number of considered nano-particles is N_p in $\left[1; 10^5\right]$ (which can be compared to experimental structures). With the selected parameters of the remeshing process, $h_{\min}$ in [0.1; 1.0] nm, $h_{\max}$ in [2.0; 20.0] nm and δ_{ϕ} in [0.001; 0.100], the number of computing nodes N_n in $\left[10^4;10^8\right]$ and the spatial positions of nodes $\left\{x_j, y_j, z_j\right\}_{j=1}^{N_n}$ are adapted in order to satisfy the maximum error δ_{ϕ} in the whole computational domain Ω.

To illustrate, we consider gold nano-particle of radius r_p in {10.0, 11.0, 12.0, 13.0} nm embeded in sourrounding medium of permittivity ε_m in {0.999, 1.000, 1.001 } illuminated at wavelength λ in {500, 501, 502, 503} nm. The gold permitivitty is $\varepsilon_p(\lambda) = \varepsilon_r(\lambda) + j\varepsilon_i(\lambda)$ and different values are considered: $\varepsilon_r(\lambda) = \left\{\varepsilon_r(\lambda) - 0.01, \varepsilon_r(\lambda), \varepsilon_r(\lambda) + 0.01\right\}$, and $\varepsilon_i(\lambda) = \left\{\varepsilon_i(\lambda) - 0.01,\ \varepsilon_i(\lambda),\ \varepsilon_i(\lambda) + 0.01\right\}$. With such physical parameters and the remeshing parameters $h_{\min} = 0.1\ \text{nm}$, $h_{\max} = 20.0\ \text{nm}$ and $\delta_{\phi} = 0.05$, the total number of nodes is $N_n = 243200$, producing sequences $\Psi_{\text{out}}(n)$ of 1,945,600 bits. Therefore, the total number of generated sequences is $N_k = 432$ (corresponding to 4 values of r_p, 4 values of λ, 3 values of ε_m, 3×3 values for both real and imaginary parts of ε_p). Each sequence has a size of 1,945,600 bits. The produced maps $I_E(x,y,z)$, $X_E(n)$ (resp. $I_H(x,y,z)$, $X_H(n)$) and $\Psi_{\text{out}}(n)$, can be viewed as vectors made up of all the numbers of nodes ranked in a precise order. Moreover, the elements of these vectors can be viewed on a 2D map (*i.e.* the corresponding images in gray levels of the generated maps, see **Figure 1**). **Figure 1** shows an example of the corresponding 2D images of the maps $I_E(x,y,z)$, $I_H(x,y,z)$, $X_E(n)$, $X_H(n)$ and the pseudo random sequence $\Psi_{\text{out}}(n)$. The **Figures 1(a)** and **(b)** let appear low structures and have low Shannon's entropy. This mainly comes from the fact that there are many missing levels of intensities. We also remark the non regularity in the occurency of the zero-bit value (0) relatively to one-bit value (1) in the corresponding binary sequence of this image (62.51% against 37.49% for the image of **Figure 1(a)**). The output sequence $\Psi_{\text{out}}(n)$, obtained after a xor operation between $X_E(n)$ and $X_H(n)$, presents the characteristics of randomnes (see **Figure 1(e)**) and pass all the NIST tests successfully (see Section 3.2.1).

3.2. Statistical Analysis

In order to analyse the qualities of the produced pseudo random sequences, two approaches are developped and used. These qualities are investigated following both aspects: randomness properties of the individual sequences and correlation between multiple sequences.

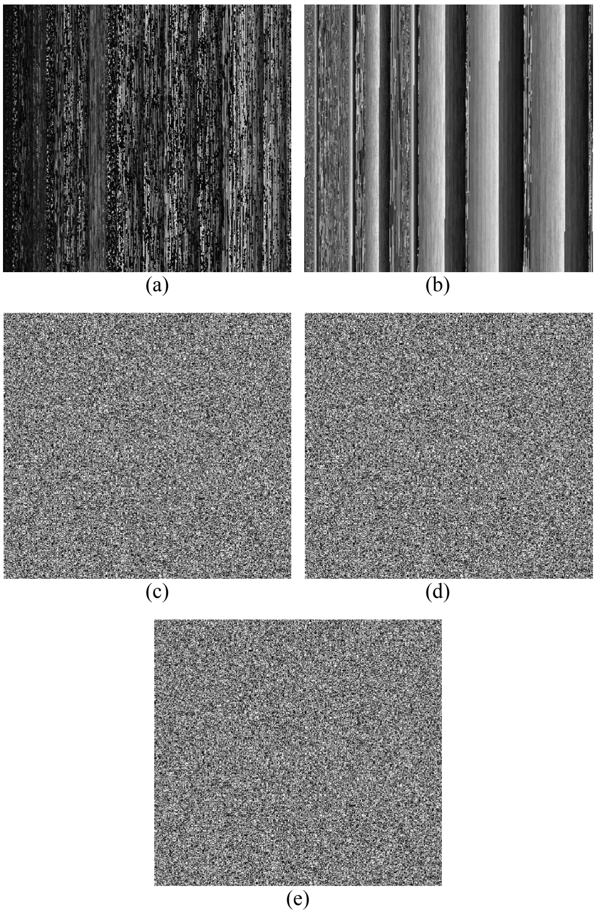

(a) (b)
(c) (d)
(e)

Figure 1. The corresponding 2D images, in gray levels, of the maps (a) $I_E(x,y,z)$, (b) $I_H(x,y,z)$, (c) $X_E(n)$, (d) $X_H(n)$ obtained after renumbering, homogenization and projection in basis *C*. The map (e) $\Psi_{\text{out}}(n)$ is obtained from the xor operator between $X_E(n)$ and $X_H(n)$. The total size of each image is 243,200 pixels (475×512), each pixel being expanded on 8 bytes (256 levels).

3.2.1. Randomness Analysis

The goal of this approach is to evaluate the randomness level of the sequences Ψ_{out} produced by the algorithm. The sequences are evaluated through statistical tests suite NIST (National Institute of Standards and Technology of the US Government). The NIST statistical test battery have been chosen for the following reasons. Firstly, it contains many famous tests from the Diehard battery with some extra tests. Secondly, it was used in the AES evaluation process to check the randomness of the output sequences of each candidate algorithm. Moreover, the NIST tests have also shown their ability to ckeck pseudo random number generators in smart cards [22]. This NIST suite consists in a statistical package of fifteen tests developped to quantify and to evaluate the randomness of (arbitrarily long) binary sequences produced by either hardware or sotware based cryptographic random or pseudo random number generators [16]. For each statistical test, a set of p_{value} is produced and is compared to a fixed significance level $\alpha = 0.01$ (*i.e.* only 1% of the sequences are expected to fail). Therefore, a sequence passes a statistical test for $p_{\text{value}} \geq \alpha$ and fails otherwise. In case of testing multiple sequences at the same time, each test define a proportion η as the ratio of sequences passing succesfully the test relatively to the total number of sequences N_k (*i.e.* $\eta = n\left[p_{\text{value}} \geq \alpha\right]/N_k$). This proportion η is compared to an acceptable proportion η_{accept} which corresponds to the ratio of sequences which should pass the test [16]. These NIST tests are achieved on the two following kind of sequences: individual sequences and the concatened sequence.

1) Individual sequences: The randomness level of each sequence belonging to a subset of sequences is analysed directly by NIST tests. The N_k sequences Ψ_{out}^k of binary size M (with $1 \leq k \leq N_k$) are individually tested and the results are given as ratio of success η compared to a fixed threshold. The provided information is the randomness of each sequence.

2) Concatened sequence: A new sequence is constructed by concatening all the individual sequences: $\Psi_{\text{cat}} = \left\{\Psi_{\text{out}}^1 \cdots \Psi_{\text{out}}^{N_k}\right\}$ of binary size $N_k \times M$. The randomness quality of this new sequence is also analysed directly by the NIST tests. The provided information is the randomness of the concatened sequence and especially the binary correlation between the produced sequences.

The results obtained on the 432 sequences are given in **Table 1**. We notice that the results of the tests are satisfactory for the whole set of tested outputs. The sequences pass successfully the NIST tests for individual sequences and for the constructed concatened sequence. These results show the quality of the produced sequences with the PRNG.

3.2.2. Correlation Analysis

In this second approach the purpose is to check the correlation between the produced pseudo random sequences. Compared to the previous approach (Approach 1.2), the correlation between sequences are analysed globally by computing the correlation coefficients of each pair of sequences [23]. Let the two sequences $x = \left[x_1, \cdots, x_N\right]$ and $y = \left[y_1, \cdots, y_N\right]$, we have:

$$C_{xy} = \frac{\sum_{i=1}^{N}\left(x_i - \bar{x}\right)\cdot\left(y_i - \bar{y}\right)}{\left[\sum_{i=1}^{N}\left(x_i - \bar{x}\right)^2\right]^{1/2}\cdot\left[\sum_{i=1}^{N}\left(y_i - \bar{y}\right)^2\right]^{1/2}}, \quad (6)$$

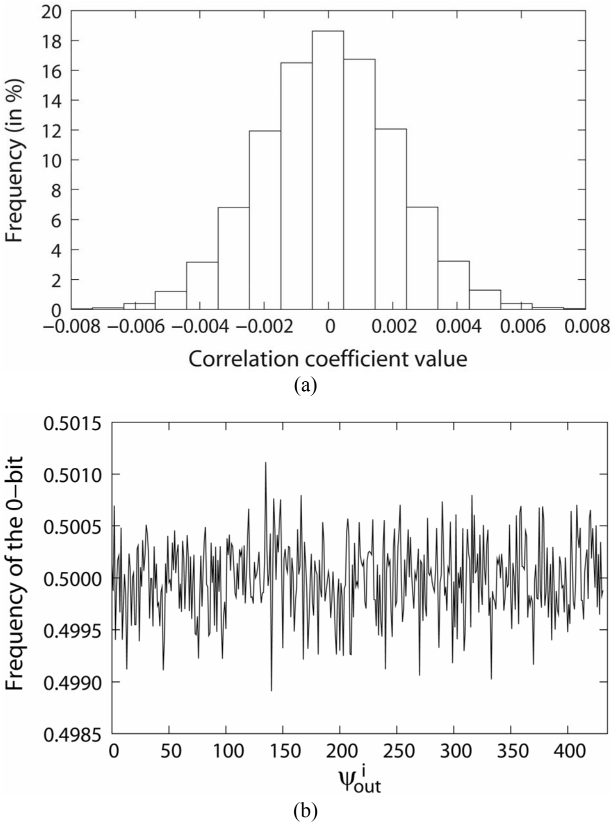
where $\bar{x} = \sum_{i=1}^{N} x_i/N$ and $\bar{y} = \sum_{i=1}^{N} y_i/N$ are the mean values of x and y, respectively. A strong correlation occurs between two sequences for $C_{xy} \simeq \pm 1$ and no

Table 1. Results of the NIST tests using Approach 1 on the 432 generated individual sequences and on the concatened sequence. The ratio η of p_{value} concerns the individual sequences while the p_{value} concerns the concatened sequence.

Test Name	Individual Sequence Ψ_{out}		Concatened Sequence Ψ_{cat}	
	η	Result	p_{value}	Result
Frequency	99.07	Pass	0.654	Pass
Block-Frequency	98.61	Pass	0.848	Pass
Cumulative Sums (1)	99.53	Pass	0.626	Pass
Cumulative Sums (2)	99.07	Pass	0.973	Pass
Runs	99.30	Pass	0.486	Pass
Longest Run	98.14	Pass	0.232	Pass
Rank	98.38	Pass	0.743	Pass
FFT	99.07	Pass	0.109	Pass
Non-Overlapping	97.98	Pass	0.109	Pass
Overlapping	99.07	Pass	0.091	Pass
Universal	99.53	Pass	0.204	Pass
Approximate Entropy	99.76	Pass	0.566	Pass
Random Excursions	98.37	Pass	0.150	Pass
Random E-Variant	97.39	Pass	0.147	Pass
Serial (1)	99.30	Pass	0.344	Pass
Serial (2)	99.07	Pass	0.232	Pass
Linear Complexity	98.14	Pass	0.856	Pass

correlation corresponds to $C_{xy} = 0$. The coefficients C_{xy} are computed for each pair of sequences and the distribution of their values is presented by a histogram. Therefore the coefficients of correlation between each pair of the 432 generated sequences are computed and the distribution of these coefficients $C_{\Psi_{\text{out}},\Psi'_{\text{out}}}$ is presented in **Figure 2**.

The result exhibits a very weak correlation between the sequences and $\max\left[C_{\Psi_{\text{out}},\Psi'_{\text{out}}}\right]$ in [–0.008; 0.008]. This confirms the decorrelation and the randomness quality of the tested individual sequences. Finally, we show, on **Figure 2(b)**, the distribution of occurencies of the 0-bit for each produced pseudo random sequence. This distribution is uniform around the value 0.50. Each sequence Ψ^i_{out} ($1 \le i \le 432$) can be now viewed as a pseudo random octal sequence. The outputs of PRNG must have both strong quality of randomness and strong independence between these outputs. The results of the analysis, obtained with the two approaches, show the randomness level of the pseudo random sequences and the quasi independence that may exist between a group of produced pseudo random sequences.



(a)

(b)

Figure 2. (a) Histogram of distribution of the correlation coefficients $C_{\Psi_{\text{out}},\Psi'_{\text{out}}}$ on the interval $[-0.008;0.008]$; (b) Distribution of the 0-bit in the generated pseudo random sequences $\Psi^i_{\text{out}}, 1 \le i \le 432$.

3.3. Security Analysis

The security analysis of any PRNG should also be evaluated against attacks as well as its application domain. Therefore, the analysis must take into account all the critical points of the cryptosystem and must meet cryptographic requirements [24]. In the present case, the investigated points are: the size of the key space, the key sensitivity, the randomness quality of the ouputs. These points are investigated through the two following attacks: Heuristic Guess-and-Determine Attack [25], Distinguishing Attack [26].

3.3.1. Key Space

A good generator of (pseudo) random sequences should have a large key space in order to make brute-force attacks infeasible. It is generally accepted that a key space of size smaller than 2^{128} is not secure enough [21]. The theoretical size of the key space given in the (Section 2) is $\mathbb{N}\times\mathbb{R}^{5+4N_p}\times\mathbb{C}^{1+N_p}$ or $\mathbb{N}\times\mathbb{R}^{5+4N_p}\times\mathbb{C}^{2+2N_p}$. For $N_p = 1$, the theoretical entropy of the key space is equal to 448. For real physics measurements, the size of the space of input parameters is smaller. Indeed, the parameters do not take all the possible values in $\mathbb{N}$, $\mathbb{R}$ or $\mathbb{C}$, which can decrease the size of the key space. In fact, with such limitation of parameter space, we already assure to be in the region of near-field inducing plasmonic effects (*i.e.* strong resonances and interference patterns in the electromagnetic field). For example, by taking into account the available physical measures (see the sizes of intervals for each parameter given in Section 3.1), the values of parameters can be limited at least on a 12- to 16-bits encoding. With such limited bits encoding, the entropy of the key space is 156 bits (or 224 bits for a 16-bits encoding) with only one considered nano-sphere (*i.e.* $N_p = 1$). This clearly overpass the lower limit of 128 bits. Therefore, the size of the key space is large enough to resist brute-force attacks. Such a large space of keys is a necessary condition, but not sufficient. Indeed, all the keys must be equiprobable and the corresponding outputs must also be cryptographically strong.

3.3.2. Key Sensitivity

The sensitivity on the key is an essential factor for the pseudo random generation based on optical system. Indeed, only a small deviation in the input should cause a large change in the output. Here, the key is given by various kinds of inputs (physical parameters) such as the radius of the nano particle r_p, the permittivity of the materials ε_p, the number of particles N_p, the permittivity of the surrounding medium ε_m, the illuminating angle θ_i and the illuminating wavelength λ. The numerical parameters (*i.e.* $h_{\min}$, $h_{\max}$ and δ_ϕ) define the length of the pseudo random sequences (N_n)

and the spatial positions where the fields are computed ((x_i, y_i, z_i) , with $1 \le i \le N_n$). The key sensitivity analysis must be normally achieved on all these parameters (physical and numerical parameters). Neverthless, the main sensitive parameters concern physical ones. Therefore, we can limit this analysis to mainly four physical parameters: the radius of the nano-particles r_p, the surrounding medium ε_m, the complex permitivitty ε_p (*i.e.* the real and imaginary parts $\varepsilon_p = \varepsilon_r + j\varepsilon_i$) of the nano-particle material and the illuminating wavelength λ.

Actually, in the study of correlation (Section 3), the sensitivity was already indirectly tested due to the selected near values of input parameters. Here, the analysis is achieved on individual physical parameters in order to analyse the sensitivity of these parameters through the computing of the correlation coefficient values. To analyse the sensitivity to the physical parameters, we consider the generation of large pseudo random sequences Ψ_{out} of size $N_n = 243,200$ (*i.e.* $M = 1,945,600$ bits with $h_{\min}$ = 0.1 nm, $h_{\max} = 20.0$ nm and $\delta_\phi = 0.05$) obtained for $N_p = 1$ spherical nanoparticle.

1) Radius Value Sensitivity:

The first parameter concerns the radius r_p of the nano-particle. The fixed parameters are: the permittivity of the surrounding medium $\varepsilon_m = 1.000$, the permittivity of the gold nano-sphere $\varepsilon_p = -2.6252 + j3.5563$ at the illuminating wavelength $\lambda = 501$ nm . With three slightly differing radius values $r_p^a = 10$, $r_p^b = 11$ and $r_p^c = 12$, the produced sequences are Ψ_{out}^a, Ψ_{out}^b and Ψ_{out}^c, respectively. If the cryptosystem is sensitive to the radius value then the produced outputs Ψ_{out}^a and Ψ_{out}^c should be very different from Ψ_{out}^b and not correlated. The correlation coefficients between these three produced sequences are presented in **Table 2**. The produced sequences Ψ_{out}^a, Ψ_{out}^b and Ψ_{out}^c are very different for near radius r_p values and only a very weak correlation is detected.

2) Surrounding Medium Permittivity Value Sensitivity:

The second parameter is the value of the surrounding medium permittivity ε_m. The fixed parameters are: the radius of the nano-sphere $r_p = 11$ nm , the permittivity of the gold nano-sphere $\varepsilon_p = -2.6252 + j3.5563$ at the illuminating wavelength $\lambda = 501$ nm . With these fixed parameters and the three slightly differing permittivity values $\varepsilon_m^a = 0.999$, $\varepsilon_m^b = 1.000$ and $\varepsilon_m^c = 1.001$, the produced sequences are Ψ_{out}^a, Ψ_{out}^b and Ψ_{out}^c, respectively. The correlation coefficients between these three produced sequences are presented in **Table 3**. For near permittivity values ε_m, the produced sequences Ψ_{out}^a, Ψ_{out}^b and Ψ_{out}^c are also different and only a weak correlation is detected.

3) Sensitivity of the real part of the material permitivity:

Table 2. Correlation coefficients between the three pseudo random sequences produced with slightly different radius values r_p^a, r_p^b and r_p^c.

Outputs 1/2	$\Psi_{\text{out}}^a/\Psi_{\text{out}}^b$	$\Psi_{\text{out}}^a/\Psi_{\text{out}}^c$	$\Psi_{\text{out}}^b/\Psi_{\text{out}}^c$
Corr. Coef.	0.00136	–0.00022	0.00094

Table 3. Correlation coefficients between the three pseudo random sequences produced with slightly different surrounding medium values ε_m^a, ε_m^b and ε_m^c.

Outputs 1/2	$\Psi_{\text{out}}^a/\Psi_{\text{out}}^b$	$\Psi_{\text{out}}^a/\Psi_{\text{out}}^c$	$\Psi_{\text{out}}^b/\Psi_{\text{out}}^c$
Corr. Coef.	–0.00233	0.00060	0.00061

The third parameter is the value of the real part of the complex permittivity of the gold nano-particle ε_r. The fixed parameters are: the radius of the nano-sphere $r_p = 11$ nm , the permittivity of the surrounding medium $\varepsilon_m = 1.000$ and the imaginary part of the permittivity of gold nano-sphere $\varepsilon_i = 3.5563$ at the illuminating wavelength $\lambda = 501$ nm . With these fixed parameters and the three slightly differing real part of the permittivity values $\varepsilon_r^a = -2.6152$, $\varepsilon_r^b = -2.6252$ and $\varepsilon_r^c = -2.6352$, the produced sequences are Ψ_{out}^a, Ψ_{out}^b and Ψ_{out}^c, respectively. The correlation coefficients between these three produced sequences are presented in **Table 4**. The cryptosystem is also sensitive to the value of real part of the material permitivitty.

4) Sensitivity to the imaginary part of the material permittivity:

The fourth parameter is the value of the imaginary part of the complex permittivity of the gold nano-particle ε_i. The fixed parameters are: the radius of the nano-sphere $r_p = 11$ nm , the permittivity of the surrounding medium $\varepsilon_m = 1.000$ and the real part of the permittivity of gold nano-sphere $\varepsilon_r = -2.6252$ at the illuminating wavelength $\lambda = 501$ nm . With these fixed parameters and the three slightly differing imaginary part of the permittivity values $\varepsilon_i^a = 3.5463$, $\varepsilon_i^b = 3.5563$ and $\varepsilon_r^c = 3.5663$, the produced sequences are Ψ_{out}^a, Ψ_{out}^b and Ψ_{out}^c, respectively. The correlation coefficients between these three produced sequences are presented in **Table 5**. The tested sequences Ψ_{out}^a , Ψ_{out}^b and Ψ_{out}^c are uncorrelated. The cryptosystem is sensitive to the value of imaginary part of the material permitivitty.

5) Illuminating wavelength value sensitivity:

The last parameter concerns the illuminating wavelength values λ. The fixed parameters are: the radius of the nano-sphere $r_p = 11$ nm , the permittivity of the surrounding medium $\varepsilon_m = 1.000$ and the complex permittivity of gold nano-sphere $\varepsilon_p = -2.6252 + j3.5563$. With these fixed parameters and the three slightly differing illuminating wavelength $\lambda^a = 500$, $\lambda^b = 501$

Table 4. Correlation coefficients between the three pseudo random sequences produced with slightly different values of ε_r^a, ε_r^b and ε_r^c retated to the real part of the permitivitty of gold nanosphere.

Outputs 1/2	$\Psi^a_{\text{out}}/\Psi^b_{\text{out}}$	$\Psi^a_{\text{out}}/\Psi^c_{\text{out}}$	$\Psi^b_{\text{out}}/\Psi^c_{\text{out}}$
Corr. Coef.	–0.00218	–0.00022	–0.00062

Table 5. Correlation coefficients between the three pseudo random sequences produced with slightly different values of ε_i^a, ε_i^b and ε_i^c retated to the imaginary part of the permitivitty.

Outputs 1/2	$\Psi^a_{\text{out}}/\Psi^b_{\text{out}}$	$\Psi^a_{\text{out}}/\Psi^c_{\text{out}}$	$\Psi^b_{\text{out}}/\Psi^c_{\text{out}}$
Corr. Coef.	0.00066	–0.00288	0.00312

and $\lambda^c = 502$, the produced sequences are Ψ^a_{out}, Ψ^b_{out} and Ψ^c_{out}, respectively. The correlation coefficients between these three produced sequences are presented in **Table 6**.

Table 6. Correlation coefficients between the three pseudo random sequences produced with slightly different wavelength values λ_a, λ_b and λ_c.

Outputs 1/2	$\Psi^a_{\text{out}}/\Psi^b_{\text{out}}$	$\Psi^a_{\text{out}}/\Psi^c_{\text{out}}$	$\Psi^b_{\text{out}}/\Psi^c_{\text{out}}$
Corr. Coef.	0.00169	0.00107	–0.00077

These coefficients are closed to 0 then the tested outputs are very different. The results obtained here show that the sequences seem to be very different and also illustrate the sensitivity of the cryptosystem relatively to the wavelength value.

3.3.3. Quality of Pseudo Random Sequences

A mathematical analysis would be necessary to determine is the PRNG is robust or not before being used. Indeed, whichever way the cryptosystem is designed, the produced output must be strong (*i.e.* random, decorrelated and sensitive). Several and various statistical tests are available for evaluating the randomness of binary sequences. Reference test suites for PRNGs are the NIST suite [16], TestU01 [27] and the DieHARD suites [28]. In this paper, the NIST tests are used to evaluate the randomness level of subset of pseudo random sequences. As previously mentionned, the NIST statistical test battery are chosen because it contains many famous tests from the Diehard battery with some extra tests and used to check the randomness of the output sequences of each candidate algorithm in the AES evaluation process and smart cards [22]. The correlation between such pseudo random sequences was also evaluated (see Statistical analysis in Section 3.2). The sensitivity to the parameters of the key (λ, r_p, ε_p, ε_m) was also analysed. All the produced pseudo random sequences pass successfully the tests.

3.3.4. Security against Attacks

We also analyse the security of the cryptosystem against two types of attacks: Heuristic Guess-and-Determine Attack and Distinguishing Attacks.

1) Heuristic Guess-and-determine (HGD) attack is a general attack on stream ciphers [25]. The main idea of this attack is to guess in the first time the value of few unknown variables of the cipher. Next, the remaining unknown variables are deduced by iterating the system a few times and by comparing the produced pseudo random sequence with the original pseudo random sequence. If these two sequences are equal, then the guessed values are correct and the cryptosystem is broken, else the attack should be repeated with new guessed values. We consider that the system is known by the attacker, it seems that the attack discussed in reference [25] can not be applied correctly on the proposed cryptosystem which is not of the same family of involved stream ciphers. In fact, the model and the structure of the proposed PRNG is completely different. An alternative way to apply this attack would be to guess and to fix the values of physical parameters and to iterate the algorithm by searching the remeshing ones to produce the sequence Ψ_{out}. Once all the comparisons made without success, the first set of input values is guessed again and the process is repeated until success. This process has almost the same complexity than a classic brute-force attack.

2) Distinguishing Attacks: Any output of a stream cipher (or PRNG) designed for cryptographic applications, should not be statistically distinguished from a truly random sequence. In fact, distinguishing attacks described in reference [26], try to find traces of the distinguishing property by exploiting the weaknesses of the algorithm related to the linear and non-linear combinations. Here, the generated sequences pass successfully the standard statistical tests for randomness. Moreover, the only linear masking occurs when we applied $\left[\text{Int}\left(\alpha\left|I_E(n)\right|\right)\right]$ and $\left[\text{Int}\left(\alpha\left|I_H(n)\right|\right)\right]$ in Equations (3) and (4). Knowing that the values of $I_E(n)$ and $I_H(n)$ are sensitive from the second or third decimal place, the fact to mulltiply by α gives values which the modulo are completely different. Thus, by applying a XOR operation between the two maps $X_E(n)$ and $X_H(n)$ it kills any information on linear dependance then, the attack becomes ineffective.

4. Conclusion

In this paper, a new PRNG using two plasmonic maps to generate long pseudo random sequences was presented. Such a generator has shown its ability to produce a very large number of pseudo random sequences which can be usefull in several cryptographic applications. The randomness quality on the plasmonic maps is improved through the use of remeshing process and one-way function (xor operator). The advantages of the generator are the size of the key space, the sensitivity to the initial inputs (keys), the quality of pseudo random sequences and the security level against several attacks. Moreover, these produced sequences do not present correlations which ensuring a large variety of pseudo random sequences and a higher security level. Of course, this method can be enriched by increasing the complexity of the nanostructures (including substrates, multi-materials, ...) inducing complex interaction patterns and strong gradients and by considering experimental field measurements.

5. Acknowledgements

Authors thank the Centre de Calcul Intensif ROMEO II for computational facilities, the Région Champagne-Ardennes and the Conseil Régional de l'Aube for financial supports.

REFERENCES

[1] L. Blum, M. Blum and M. Shub, "A Simple Unpredictable Pseudo-Random Number Generator," *SIAM Journal on Computing*, Vol. 15, No. 2, 1986, pp. 364-383. doi:10.1137/0215025

[2] K. W. Wojciechowski, "Pseudorandom Number Generators Based on the Weyl Sequence," *Computational Methods in Science and Technology*, Vol. 5, 1999, pp. 81-85.

[3] N. K. Pareek, V. Patidar and K. K. Sud, "Discrete Chaotic Cryptography Using External Key," *Physics Letters A*, Vol. 309, No. 1-2, 2003, pp. 75-82. doi:10.1016/S0375-9601(03)00122-1

[4] 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, 2009, pp. 327-344.

[5] S. M. Fu, Z. Y. Chen and Y. A. Zhou, "Chaos-Based Random Number Generators," *Computer Research and Development*, Vol. 41, No. 4, 2004, pp. 749-754.

[6] J. P. Gonzailez and R. Pino, "Random Number Generator Based on Unpredictable Chaotic Functions," *Computer Physics Communications*, Vol. 120, No. 2-3, 1999, pp. 109-114. doi:10.1016/S0010-4655(99)00233-7

[7] V. V. Kolesov, R. V. Belyaev and G. M. Voronov, "A Digital Random-Number Generator Based on the Chaotic Signal Algorithm," *Journal of Communications Technology and Electronics*, Vol. 46, No. 11, 2001, pp. 1258-1263.

[8] F.-L. Wang, "A Universal Algorithm to Generate Pseudo-Random Numbers Based on Uniform Mapping as Homeomorphism," *Chinese Physics B*, Vol. 19, No. 19, 2010, p. 090505.

[9] I. Vattulainen, K. Kankaala, J. Saarinen and T. Ala-Nissila, "A Comparative Study of Pseudo-Random Number Generators," *Computer Physics Communications*, Vol. 86, No. 3, 1995, pp. 209-226. doi:10.1016/0010-4655(95)00015-8

[10] A. B. O. López, G. Á. Marañon, A. G. Estévez, G. P. Dégano, M. R. García and F. M. Vitini, "Trident, a New Pseudo-Random Number Generator Based on Coupled Chaotic Maps," *Advances in Intelligent and Soft Computing*, Vol. 85, 2010, pp. 183-190. doi:10.1007/978-3-642-16626-6_20

[11] N. K. Pareek, V. Patidar and K. K. Sud, "A Random Bit Generator Using Chaotic Maps," *International Journal of Network Security*, Vol. 10, No. 1, 2010, pp. 32-38.

[12] D. Barchiesi, D. Macías, L. Belmar-Letellier, D. van Labeke, M. Lamy de la Chapelle, T. Toury, E. Kremer, L. Moreau and T. Grosges, "Plasmonics: Influence of the Intermediate (or Stick) Layer on the Efficiency of Sensors," *Applied Physics B-Lasers and Optics*, Vol. 93, No. 1, 2008, pp. 177-181. doi:10.1007/s00340-008-3173-5

[13] T. Grosges, D. Barchiesi, T. Toury and G. Gréhan, "Design of Nanostructures for Imaging and Biomedical Applications by Plasmonic Optimization," *Optics Letters*, Vol. 33, No. 23, 2008, pp. 2812-2814. doi:10.1364/OL.33.002812

[14] T. Grosges and D. Barchiesi, "Toward Nanoworld-Based Secure Encryption for Enduring Data Storage," *Optics Letters*, Vol. 35, No. 14, 2010, pp. 2421-2423. doi:10.1364/OL.35.002421

[15] M. François, T. Grosges, D. Barchiesi and R. Erra, "Generation of Encryption Keys from Plasmonics," *PIERS Online*, Vol. 7, No. 3, 2011, pp. 296-300.

[16] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray and S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," National Institute of Standard Technologies Special Publication, Washington DC, 2010, pp. 1-200.

[17] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, Vol. 27, No. 3-4, 1948, pp. 379-423, 623-656.

[18] D. Barchiesi, E. Kremer, V. P. Mai and T. Grosges, "A Poincaré's Approach for Plasmonics: The Plasmon Localization," *Journal of Microscopy*, Vol. 229, No. 3, 2008, pp. 525-532. doi:10.1111/j.1365-2818.2008.01938.x

[19] H. Borouchaki, T. Grosges and D. Barchiesi, "Improved 3D Adaptive Remeshing Scheme Applied in High Electromagnetic Field Gradient Computation," *Finite Element in Analysis and Design*, Vol. 46, No. 1-2, 2010, pp. 84-95. doi:10.1016/j.finel.2009.06.026

[20] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography," CRC Press, Boca Raton, 1996. doi:10.1201/9781439821916

[21] W. Janke, "NIC Series Volume 10: Quantum Simulations of Complex Many-Body Systems: From Theory to Algorithms," John von Neumann Institute for Computing, Kerkrade, 2002, pp. 447-458.

[22] R. N. Akram, K. Markantonakis and K. Mayes, "Pseudorandom Number Generation in Smart Cards: An Implementation, Performance and Randomness Analysis," *The*

5th International Conference on New Technologies, *Mobility and Security* (*NTMS*), Istanbul, 7-10 May 2012, pp. 1-7. doi:10.1109/NTMS.2012.6208760

[23] G. Cheng, Y. Mao and C. Chui, "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps," *Chaos Solitons and Fractal*, Vol. 21, No. 3, 2004, pp. 749-761. doi:10.1016/j.chaos.2003.12.022

[24] G. Alvarez and L. Shujun, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems," *International Journal of Bifurcation and Chaos*, Vol. 16, No. 8, 2006, pp. 2129-2151. doi:10.1142/S0218127406015970

[25] H. Ahmadi and T. Eghlidos, "Heuristic Guess-and-Determine Attacks on Stream Ciphers," *IET Information Security*, Vol. 3, No. 2, 2009, pp. 66-73. doi:10.1049/iet-ifs.2008.0013

[26] D. Coppersmith, S. Halevi and C. Jutlar, "Cryptanalysis of Stream Ciphers with Linear Masking," *CRYPTO* '02 *Proceedings of the* 22*nd Annual International Cryptology Conference on Advances in Cryptology*, Vol. 2442, 2002, pp. 515-532.

[27] P. L'ecuyer and R. Simard, "TestU01: A C Library for Empirical Testing of Random Number Generators," *ACM Transactions on Mathematical Software*, Vol. 33, No. 4, 2007, pp. 22-40.

[28] G. Marsaglia, "Diehard: A Battery of Tests of Randomness," 1996. http://stat.fsu.edu/geo/diehard.html