ON SOME MODELS OF PSEUDORANDOM NUMBER GENERATORS BASED ON CHAOTIC DYNAMICAL SYSTEMS

Janusz Szczepański, Zbigniew Kotulski
Polish Academy of Sciences, Institute of Fundamental Technological Research
Świętokrzyska 21, 00-049 Warsaw, Poland
E-mail: jszczepa@ippt.gov.pl.
Karol Górski, Andrzej Paszkiewicz, Anna Zugaj
Warsaw University of Technology, Institute of Telecommunications
Nowowiejska 15/19, 00-665 Warsaw, Poland
E-mail: karol@tele.pw.edu.pl.

KEYWORDS

Pseudorandom numbers generators, stream ciphers, dynamical systems, chaos, ergodicity, statistical tests.

ABSTRACT

Pseudorandom number generators (PNG) are frequently used in many areas of contemporary technic like engineering applications as well as modern communication systems. In recent years a new approach to construct save cryptosystems based on application of the theory of both continuous and discrete chaotic dynamical systems is developed. Within the continuous theory methods of synchronization of chaotic systems and idea of controlling chaos are applied.

In this paper we present some models of pseudorandom number generators construction of which is based on discrete chaotic dynamical systems. The principal feature of chaos is that simple deterministic nonlinear systems can generate trajectories which appear to be "random". The randomness is a consequence of extreme sensitivity of the trajectories to small changes of initial conditions. This means in fact that it is not possible to reconstruct them without knowledge precise initial conditions. The basic idea of construction of chaotic pseudorandom number generators (CPNG) strongly explores this property since the bits generated are associated in some appropriate way with a behaviour of the trajectories. To assure a good statistical properties (which decide about the quality of a generator) of CPNG we shall assume that the dynamical systems used are also ergodic or preferably mixing. This allow us to make use of the well developed theory of dynamical systems to prove the required statistical properties.

Finally, since chaotic systems often appear in realistic physical situations we propose some physical realisations of CPNG.

INTRODUCTION

Pseudorandom numbers with "good" properties are frequently used for a variety of engineering applications as well as in modern communication systems. Quality in this case may be defined by how well the given device or algorithm for producing the random or pseudorandom numbers imitates an ideal source of uniformly distributed and independent random numbers. Many cryptographic schemes and protocols require a source of random or pseudorandom numbers. The quality of this source is crucial for the security of the scheme or protocol.

Traditionally, extensive statistical testing was used to assess or estimate this quality. (Possession of a good pseudorandom bit generator (PBG) is sufficient to construct a good pseudorandom number generator and it is often easier to work with bit generators.) Test suites developed for this purpose may be found in [Knuth81], [Beker82], [FIPS94]. For example, FIPS 140-1 specifies the following 4 tests on sequences of 20000 bits:

1. the monobit test - the number of one bits in the sequence must lie between specified limits,
2. the poker test - the histogram of values of non-overlapping four bit segments must be resemble to the uniform distribution; in this and the previous test the chi-square test is used,
3. the runs test - the number of runs (the test is carried out for runs of zeros and runs of ones) of length 1, 2, 3, 4 and 5 as well as the number of

runs which are longer than 5 must each lie between specified limits,
4. the long run test - in the tested sequence there must be no run of length equal to or greater than 34 bits.

Additional tests used in cryptography include spectral tests, entropy tests and tests of linear, maximal order or sequence complexity profiles [Schne96].

In the case of pseudorandom number generators some a priori conditions for their acceptance were formulated by Golomb [Golo67]. His three postulates concern properties of periodic pseudorandom bit generators and refer to quantities calculated over one complete period of the generator. They are as follows:
1. the number of zero bits should differ from the number of one bits by at most one,
2. among all the runs half should be of length 1, a quarter should be of length 2, an eighth should be of length 3 and so on (as long as the number of runs so indicated exceeds one); for each of these lengths there should be equally many runs of zero bits and runs of one bits
3. the autocorrelation function is two-valued: when the offset is 0 or is a multiple of the period, the value of the autocorrelation function is equal to the period of the generator; otherwise this value is equal to a certain constant integer.

In the case of some classes of algorithmic pseudorandom number generators a further level of assurance has been obtained by a theoretical analysis of the algorithms. Linear feedback shift registers (LFSR) are a well-known example. Another example is the class of generators whose security has been linked to hard computational problems in number theory (for example the Blum-Blum-Shub generator). However, in the latter case, the theoretical results are asymptotic in nature and it is difficult to find any published numerical verification of the quality of these generators with fixed security parameters. In addition, the results rely on unproved (although widely believed) hypotheses about the computational complexity of the underlying problems. In this paper we attempt to develop a theoretical foundation for a class of generators based on chaotic and ergodic transformations.

Since last few decades, a new phenomenon called chaos [Lin84] in nonlinear systems has been discovered and intensively investigated. The principal feature of chaos is that simple deterministic systems arising in many areas can generate trajectories which appear to be random. The essential property of such systems is extreme sensitivity of the trajectories to small changes to initial conditions [Lin84]. Such properties seem to be relevant for exploring during construction of cryptographic algorithms. Therefore the theory of chaotic dynamical systems is recently extensively applied for construction of cryptographic systems (both block ciphers [Habu91] and stream ciphers [Kohda97]). The earliest applications of chaotic systems were based on encrypting messages by modulating the trajectories of continuous dynamical systems. These methods are strongly connected with the concept of synchronization of two chaotic systems [Parl92], [Peco90] and controlling chaos [Kapi96], [Ott90]. Another idea is to make use of discrete dynamical systems to construct secure cryptosystems [Kotul97], [Kotul99]. It was developed in the case of block ciphers and makes use of multiple iterations and inverse iterations of chaotic maps.

In the next section, for the sake of completeness, we recall the basic concepts of the discrete dynamical systems theory.

DISCRETE DYNAMICAL SYSTEMS

We define the discrete dynamical system as a couple (S, F), where S is the state space (usually a topological metric space) and $F: S \to S$ is a measurable map being a generator of the semigroup of iterations. The trajectory of an initial state s_0 is the set $\{s_n\}_{n=0}^{\infty}$ of elements of S obtained by iteration

$$s_{n+1} = F(s_n), \qquad n = 0,\ 1,\ 2,... \tag{1}$$

The definition of chaos is closely related to the concept of Lyapunov exponents. Let $s \in S$, v be an element of the tangent space at s and $DF^n(s)(v)$ is the Frechet derivative of the n-th iteration of F at s in the direction v. Then the Lyapunov exponent is the limit

$$\lambda_{s,v} \equiv \lim_{n\to\infty} \frac{1}{n} \ln \left\| DF^n(s)(v) \right\|, \tag{2}$$

where $\| \ \|$ is the norm in the tangent space at point s. The Lyapunov exponents exist under some general conditions concerning smoothness of F [Guck83]. The number of different Lyapunov exponents at s is at most equal to the dimension of the tangent space.

We say that the dynamical system is chaotic in some region if for almost all points (with respect to some invariant measure, equivalent to Lebesgue measure) in this region it has positive Lyapunov exponents.

Chaos in a dynamical system makes the trajectories very unstable; starting from two very close initial conditions, after some iterations, we come to quite different final states (trajectories diverge exponentially). More precisely, for a one dimensional dynamical system (R,ψ), where ψ is C^1, if at some point $x\in R$, $\lambda_x>0$ (in one dimension the direction v is determined by the space itself) then

$$\forall\varepsilon>0,\ \exists n_1,n_2,\ \exists U_{n_1,n_2}\ni x,\ \forall n_1\le n\le n_2,\ \forall z_1,z_2\in U_{n_1,n_2}$$
$$e^{(\lambda_x-\varepsilon)n}|z_1-z_2|<\left|\psi^n(z_1)-\psi^n(z_2)\right|<e^{(\lambda_x+\varepsilon)n}|z_1-z_2|. \tag{3}$$

In the above, U_{n_1,n_2} is some neighbourhood of x.

Expression (3) means that the initial distance $|z_1-z_2|$ between two arbitrary points z_1, z_2 (which are elements of the neighbourhood U_{n_1,n_2} of point x) after n iterations will increase at least $e^{(\lambda_x-\varepsilon)n}$ times. The essential point for cryptographic purposes is to select the natural numbers n_1 and n_2 (to guarantee the numerical accuracy of calculations) and then determine K_{n_1,n_2}, the set of points x considered as the secret key space, satisfying property (3) with the above natural numbers .

To introduce the concept of ergodicity we assume that for the dynamical system (S,F) there exists an F-invariant measure μ, $\mu(S)<\infty$, that is, a measure which satisfies

$$\forall A\in\sigma(S),\quad \mu(A)=\mu\left(F^{-1}(A)\right). \tag{4}$$

In the above, $\sigma(S)$ is the σ–algebra of measurable subsets of S.

In our considerations, when constructing a cryptographic algorithm, we introduce dynamical systems for which some invariant measure μ exists and is equivalent to the Lebesgue measure with its density function $0<g_1\le g(s)\le g_2$ (where $\forall A\in\sigma(S),\ \mu(A)=\int_A g(s)ds$ and g_1, g_2 are positive constants). If g_1 is close to g_2 then the measure μ is close to the uniform distribution, which is important in cryptography. This postulate requires the appropriate choice of the map F .

We say that a dynamical system (S,F) is ergodic [Corn82] if and only if it has only trivial invariant sets, i.e., if and only if either $\mu(B)=0$ or $\mu(S\setminus B)=0$, whenever B is a measurable, invariant under F, subset of the space S (the invariance of B means that $F(B)\subset B$).

Ergodicity implies that the space S cannot be divided into invariant nontrivial (with respect to the measure μ) disjoint parts. Therefore, if some trajectory starts from any point $s_0\in S$, it never localises in a smaller region, and knowing the final state of the system we can never identify the region (smaller than S) where the trajectory started.

The next important characteristic of trajectories (stronger than ergodicity) is the mixing property. A dynamical system is called mixing [Corn82] if the following condition is satisfied:

$$\lim_{n\to\infty}\mu\left(F^{-n}(A)\cap B\right)=\mu(A)\mu(B), \tag{5}$$

for every two sets $A,B\in\sigma(S)$. In the above $F^{-n}(A)$ is the pre-image of the set A under the n-th iteration of F . If we additionally assume that the measure μ is probabilistic that is, $\mu(S)=1$, then formula (5) can be written down in an equivalent form:

$$\lim_{n\to\infty}\frac{\mu\left(F^{-n}(A)\cap B\right)}{\mu(B)}=\frac{\mu(A)}{\mu(S)}\ . \tag{6}$$

We see that the part of B that after n iterations of F will be contained in A is asymptotically proportional to the volume (in the sense of the measure μ) of A in S .

The formulae (5) and (6) give the asymptotic condition for the spreading of the set B over the whole space S when iterating. It is also important to specify the speed of such phenomenon. In the case of K-systems [Corn82] the convergence is exponential

$$\left|\mu\left(F^{-n}(A)\cap B\right)-\mu(A)\mu(B)\right|\le e^{-pn}, \tag{7}$$

for all n satisfying: $n_0\le n$ (n_0 - some natural number) and some fixed $p>0$ depending on F .

The mixing property means that the trajectories of the system have a property of stochasticity. If we assume the measure μ to be a probabilistic one then the iterations of F make each set A (asymptotically) statistically independent from B. In other words, if we start our trajectory at some point $s_0\in S$ then after sufficiently many iterations we can reach any region of the space S with the same probability. This means that for any final state s_n and sufficiently large n, any initial state s_0 is μ-equiprobable.

The properties of dynamical systems like chaos, ergodicity and mixing make these systems „random" - studying finite dimensional distributions in the state space we cannot distinguish whether the system is chaotic or stochastic. Therefore the chaotic dynamical system seems to be a good candidate for a source of random numbers (bits).

CONSTRUCTION OF THE CHAOTIC GENERATOR

In this section we present application of discrete dynamical systems for construction of chaotic pseudorandom bit generators (CPBG). To assure required statistical properties of generated sequences we shall assume that except of being chaotic the systems are ergodic or even mixing.

The basic idea of construction is following. Let us assume that we have some dynamical system $F:S \to S$, where S is a state space of the system. By μ we denote normalized invariant measure of the system. The central point of construction is to divide the state space in some appropriate way into two disjoint parts S_0, S_1 such that $\mu(S_0)=\mu(S_1)=1/2$. As a seed we shall consider an initial point $s \in S' \subseteq S$, where S' is the set of acceptable seeds (usually $\mu(S')=1$). To obtain a pseudorandom sequence of bits we start observing the evolution of the system governed by F starting from s, i.e. the sequence $s_n := F^n(s)$ of iterations of the map F. The *n*-th bit b_n of generated sequence is equal to "0" if $F^n(s) \in S_0$ and to "1" otherwise. This way we obtain the infinite sequence of bits $G(s)$. Thus, we obtain the map:

$$G:S' \to \prod_{i=1}^{\infty}\{0,1\}, \tag{8}$$

such that

$$G(s)=\{b_i(s)\}_{i=1,2,\dots}=\{b_1(s),b_2(s),\dots\}, \tag{9}$$

where $\prod_{i=1}^{\infty}\{0,1\}$ is the Cartesian product of the infinite number of the two-elements set $\{0,1\}$.

PROPERTIES OF CPBG

We start by giving the theorem which guarantees that if we have two different seeds in the generator; then with probability one we obtain two different sequences of bits. Under the notation introduced in (8-9) we have the following:

Theorem 1

For each $s \in S'$ the following holds true:

$$\mu\left(G^{-1}\left(\{b_i(s)\}\right)\right)=0. \tag{10}$$

Proof.

Introduce the notation: $b_i = b_i(s)$ for a certain fixed point $s \in S'$. Define the sets:

$$A_{b_1} = F^{-1}\left(S_{b_1}\right),$$

$$A_{b_1 b_2} = F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right),$$

$$A_{b_1 b_2 b_3} = F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap F^{-3}\left(S_{b_3}\right)$$

and, generally,

$$A_{b_1 b_2 \dots b_n} = F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \dots \cap F^{-n}\left(S_{b_n}\right). \tag{11}$$

Let us remark that for each $z \in S'$

$z \in A_{b_1 b_2 \dots b_n} \Leftrightarrow b_i(z)=b_i(s),$ for $i=1,2,\dots,n$.

This follows form the fact that for $i=1,2,\dots,n$

$$F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \dots \cap F^{-n}\left(S_{b_n}\right) \subseteq F^{-i}\left(S_{b_i}\right), \tag{12}$$

and, consequently:

$$\begin{aligned} &F^i(z) \in F^i\left(F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \dots \right. \\ &\left. \dots \cap F^{-n}\left(S_{b_n}\right)\right) \subseteq F^i\left(F^{-i}\left(S_{b_i}\right)\right) = S_{b_i} \equiv S_{b_i(s)}. \end{aligned} \tag{13}$$

Moreover, we know that

$$\begin{aligned} &\mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \dots \cap F^{-n}\left(S_{b_n}\right)\right) \le \\ &\le \mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-n}\left(S_{b_n}\right)\right). \end{aligned} \tag{14}$$

Now we apply the mixing property (5) to the two sets

$$F^{-1}\left(S_{b_1}\right) \text{ and } S_{b_n}, \tag{15}$$

(the set S_{b_n} is equal to S_0 or S_1). For a given, sufficiently small $\varepsilon > 0$ we choose n_1 such that

$$\mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-n_1}\left(S_{b_{n_1}}\right)\right) \le \mu\left(F^{-1}\left(S_{b_1}\right)\right)\mu\left(S_{b_{n_1}}\right)+\varepsilon. \tag{16}$$

Since the measure μ is invariant, from (14) and (16) we obtain:

$$\begin{aligned} &\mu\left(F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \dots \cap F^{-n_1}\left(S_{b_{n_1}}\right)\right) \le \\ &\le \mu\left(S_{b_1}\right)\mu\left(S_{b_{n_1}}\right)+\varepsilon. \end{aligned} \tag{17}$$

Applying the mixing property to the sets

$S_{b_{n_2}} = S_0$ or S_1

for a certain $n_2 > n_1$ and

$$F^{-1}\left(S_{b_1}\right) \cap F^{-2}\left(S_{b_2}\right) \cap \dots \cap F^{-n_1}\left(S_{b_{n_1}}\right)$$

we have that if n_2 is sufficiently large then

$$\mu\left(F^{-1}\left(S_{b_1}\right)\cap F^{-2}\left(S_{b_2}\right)\cap\ldots\cap F^{-n_1}\left(S_{b_{n_1}}\right)\cap\ldots\cap F^{-n_2}\left(S_{b_{n_2}}\right)\right)\le$$
$$\mu\left(F^{-1}\left(S_{b_1}\right)\cap F^{-2}\left(S_{b_2}\right)\cap\ldots\cap F^{-n_1}\left(S_{b_{n_1}}\right)\cap F^{-n_2}\left(S_{b_{n_2}}\right)\right)\le$$
$$\mu\left(F^{-1}\left(S_{b_1}\right)\cap F^{-2}\left(S_{b_2}\right)\cap\ldots\cap F^{-n_1}\left(S_{b_{n_1}}\right)\right)\mu\left(F^{-n_2}\left(S_{b_{n_2}}\right)\right)+\varepsilon\le$$
$$\left(\mu\left(F^{-1}\left(S_{b_1}\right)\right)\mu\left(F^{-n_1}\left(S_{b_{n_1}}\right)\right)+\varepsilon\right)\mu\left(F^{-n_2}\left(S_{b_{n_2}}\right)\right)+\varepsilon. \qquad (18)$$

Using the invariance property of the measure μ we obtain from (18) the following inequality:

$$\mu\left(F^{-1}\left(S_{b_1}\right)\cap F^{-2}\left(S_{b_2}\right)\cap\ldots\cap F^{-n_1}\left(S_{b_{n_1}}\right)\cap\ldots\cap F^{-n_2}\left(S_{b_{n_2}}\right)\right)\le \qquad (19)$$
$$\frac{1}{2}\left(\frac{1}{2}\frac{1}{2}+\varepsilon\right)+\varepsilon.$$

Generally, using the complete induction property, we find a sequence $\{n_1,n_2,...,n_k\}$ for any k such that

$$\mu\left(A_{b_1b_2\ldots b_{n_1}\ldots b_{n_2}\ldots b_{n_k}}\right):=$$
$$\mu\left(F^{-1}\left(S_{b_1}\right)\cap F^{-2}\left(S_{b_2}\right)\cap\ldots\cap F^{-n_1}\left(S_{b_{n_1}}\right)\cap\ldots.\right.$$
$$\left.\cap F^{-n_2}\left(S_{b_{n_2}}\right)\cap..\cap F^{-n_k}\left(S_{b_{n_k}}\right)\right)\le$$
$$\left(\left(\left(\mu\left(S_{b_1}\right)\mu\left(S_{b_{n_1}}\right)+\varepsilon\right)\mu\left(S_{b_{n_2}}\right)+\varepsilon\ldots\right)\mu\left(S_{b_{n_k}}\right)+\varepsilon\right)+\varepsilon\le$$
$$\left(\left(\left(\frac{1}{2}\frac{1}{2}+\varepsilon\right)\frac{1}{2}+\varepsilon\ldots\right)\frac{1}{2}+\varepsilon\right)+\varepsilon\cdot \qquad (20)$$

Since ε can be taken arbitrarily small, we deduce from (20) that

$$\mu\left(A_{b_1b_2\ldots b_{n_1}\ldots b_{n_2}\ldots b_{n_k}}\right)\xrightarrow[k\to\infty]{}0, \qquad (21)$$

what concludes the Theorem 1.

In practice, making use of the chaotic property, i.e. strong sensitivity of the map F to small changes of the initial conditions (the seed) we have that for some appropriate partitions any two different seeds lead to completely different sequences, what is very important in applications.

To pass a statistical test the sequence generated must have certain properties controlled by the test. In the case of CPBG these properties are guaranteed by theorems concerning dynamical systems of ergodic and mixing type. As an example how the theory of dynamical system works we give several applications of it.

By ergodicity we obtain that the expected number of "0" in the generated sequence is equal to the expected number of "1". To be more precise, we can use the Birkhoff-Khinchin Ergodic Theorem [Corn82], which for our system can be written as:

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\chi_{S_0}\left(F^i(s)\right)=\int_S\chi_{S_0}d\mu=\mu\left(S_0\right), \qquad (22)$$

where χ_{S_0} is the indicator function of the set S_0. Since by our assumption $\mu\left(S_0\right)=1/2$ we obtain that in the pseudorandom sequence determined by the seed s the average number of "0" tends to $1/2$. (Moreover, since superposition of the same ergodic map is also ergodic we have that any subsequence $\left(b_{kn}\right)_{n=1,2,\ldots}$ has the above property, too.)

The mixing property, defined by the condition (5), means that any measurable set $A\subset S$ will be during iterations μ-uniformly distributed over the whole state space S. We use this property to prove the theorem which determines that the bits generated by CPBG are asymptotically independent.

Theorem 2

For a given mixing dynamical system $\left(S,F\right)$, there is a natural number k such that, for each $s\in S'$, the bits b_i, b_{i+k} are (asymptotically) independent for $i=1,2,...$.

Proof.

Introduce the notation: $H_k^n:=(F^k)^n$. For each $k,n=1,2,\ldots$ we define random variables Y_k^n in the following way:

$$Y_k^n(s):=\chi_{S_0}\left(H_k^n(s)\right)=\chi_{S_0}\left(\left(F^k\right)^n(s)\right), \qquad (23)$$

acting on the probabilistic space $\left\{S',\sigma(S'),\mu\right\}$, where $\sigma(S')$ is the σ - field of the measurable sets of the space S' and μ is the F-invariant measure. These random variables describe the bits generated by the CPBG based on the dynamical system $\left(S,F\right)$.

For every $n=1,2,\ldots$ consider the σ - fields corresponding to the random variables Y_k^n and Y_k^{n+1}. They are, respectively:

$$\sigma_k^n=\left\{\varnothing,S',F^{-nk}\left(S'_0\right),F^{-nk}\left(S'_1\right)\right\} \qquad (24)$$

and

$$\sigma_k^{n+1}=\left\{\varnothing,S',F^{-(n+1)k}\left(S'_0\right),F^{-(n+1)k}\left(S'_1\right)\right\} \qquad (25)$$

We have:

$$\mu\left(F^{-(n+1)k}(S'_\alpha)\cap F^{-nk}(S'_\beta)\right)=$$
$$\mu\left(F^{-k}\left(F^{-nk}(S'_\alpha)\right)\cap F^{-nk}(S'_\beta)\right)\approx$$
$$\mu\left(F^{-nk}(S'_\alpha)\right)\mu\left(F^{-nk}(S'_\beta)\right), \qquad (26)$$

where $\alpha,\beta=0$ or 1.

The last relation follows from the mixing property (5) and it is more precise the parameter *k* is larger. The relation (26) is in fact the definition of independence of the random variables Y_k^n and Y_k^{n+1}, what gives the conclusion of Theorem 2.

Then, taking for construction of CPBG the modified dynamical system $\left(S',H_k^1\right):=\left(S',F^k\right)$ for sufficiently large *k*, we obtain sequences of statistically independent random bits.

PHYSICAL MODELS OF CPBG

Chaotic, ergodic and mixing dynamical systems are realized by many real-life systems (e.g. electronic circuits, fluid dynamics models, economic phenomena and financial markets, population growth models, etc.). It could be promising to construct physical systems realizing our cryptographic algorithms. In this section we give a certain example: the application of non-classical reflection law models, originating from the kinetic theory of dilute gases, being the source of the concept of chaos and ergodicity.

The theory of non-classical reflection laws found its place in the literature [Babo84], [Howe85], [Ichi89], [Szcz91], [Szcz95], [Szcz98], [Szcz99]. The models describe the motion of a free particle in a bounded domain. Reflection law models are an intermediate case between the deterministic systems first considered by Schnute and Shinbrot [Schnu73], and the systems with random reflection laws [Gold85].

Non-classical reflection laws are used in modelling physical phenomena in solids as well. A certain interesting physical process governed by a non-classical reflection law was observed and investigated by Andreyev [Andr64]. He studied the motion of an electron in the neighbourhood of the boundary separating normal and superconducting phases. It was found that the electron, reflected from the superconducting phase, changes the sign of all three components of the velocity (the „anti-reflection" law), what is essentially different from the classical reflection, where only the sign of the orthogonal component is changed. An interesting step in description of the mesoscopic scale physical systems in solids [Altsh91], where the theory of the Andreyev reflection law is developed (approaching practical construction of such systems), is the recent paper of Nazarov [Naza98] devoted to the novel circuit theory of superconductivity.

To establish a reflection law model, describing the motion of a free particle in a bounded area, one must select a domain with a certain shape of the boundary and define the reflection law. (We consider two-dimensional domains.) Usually, the boundary is assumed to be a closed, sufficiently regular surface. The reflection laws describe in a macroscopic way the behaviour of the velocity of a freely moving particle during its contact with the boundary of the domain. The reflection law is a one-dimensional, easy to construct dynamical system possessing the required properties [Kosj72]. It can be written symbolically as:

$$v_{ref}:=T_x(v_{inc})\,, \tag{27}$$

where v_{inc} is the incoming velocity of the particle at the boundary point *x*, and v_{ref} is the velocity of the particle after the reflection.

In our model the chaos property of the reflection law is transferred to the dynamical system describing the motion of a particle. (Problems of transferring some imposed properties of dynamical system to its extension appear in various situations and are extensively investigated.) Thus, the security of the cryptosystem based on unpredictability of the location of a moving particle is assured by its chaotic behavior [Beck90], [Kotul99].

In order to get the simplest form of equations of particle motion, we use the co-ordinate system $\left(x_n,v_n\right)$, introduced by Birkhoff, where x_n denotes the position of the particle on the boundary at the moment of the *n*-th reflection, and v_n is the angle between the velocity of the particle after the reflection and the tangent to the boundary at x_n [Szcz91]. In the case of a fixed plane domain we obtain a two-dimensional discrete dynamical system $F_T(.,.)$ whose properties are dependent functionally on the reflection law $T_x(.)$. Thus, $F_T(.,.)$ acts from the product of two intervals onto the same product:

$$F_T\colon\left[0,L\right)\times\left(0,\pi\right)\to\left[0,L\right)\times\left(0,\pi\right) \tag{28}$$

and can be written in the following form:

$$\left(x_{n+1},v_{n+1}\right)=F_T(x_n,v_n)\,. \tag{29}$$

The symbol *L* in (28) denotes the length of the boundary of the domain.

Now we adopt our reflection law model to the general scheme of the chaotic random bits generator. First, the state space *S* is the Cartesian product of two intervals:

$$S=\left[0,L\right)\times\left(0,\pi\right). \tag{30}$$

The most important decision in this construction is the choice of the sets S_0, S_1. Observing histograms of the moving particle we identify the invariant measure μ of this dynamical system. In further considerations we normalise this measure to 1. It is known that such a measure is close to the Lebesgue measure on S, but is not exactly equal to it. To have the opportunity to use ergodic theory we choose the sets S_0, S_1 in such a way that

$$\mu(S_0)=\mu(S_1)=\frac{1}{2}. \qquad (31)$$

In our investigations we assumed

$$S_0=\left\{(x,v)\in S, |x|<\frac{L}{2}\right\}. \qquad (32)$$

We start observation of the evolution of the particle starting from an initial state (x_0,v_0), playing the role of the seed. We generate a sequence of bits by taking the n-th bit equal to „0" if the state of the particle is at the moment of the n-th reflection in the set S_0, that is $(x_n,v_n)\in S_0$, and „1" otherwise.

In practice, users of a stream cryptosystem need a large number of sequences. We can generate them by changing the initial conditions of the particle (the seed). Using the mixing property (provided by transferring phenomenon) of the reflection law models we proved that the bits generated are statistically independent. Moreover, by chaos we obtained, that two sequences corresponding to two different seeds are different and cannot overlap over long subsequences of bits.

Although the correctness of the results is guaranteed by the general theory, the results are asymptotic and practical application of the theoretical construction presented above should be statistically verified.

FINAL REMARKS

In the paper we presented the construction of generator of pseudorandom sequences based on the theory of dynamical systems. We showed that statistical properties of sequences generated by them are sufficiently good for cryptographic purposes.

Generating bits according to some algorithm one requires complete repeatability (which is a necessary condition of correct decryption in the stream cipher methods). In practical implementations the numbers used in calculations are expressed with some accuracy. Therefore, when the state $F^n(s)$ is close to the boundary of separation of sets S_0 and S_1, then the numerical error can make that "0" generated in one computer become "1" in another (or vice versa). The idea how to prevent this inconvenience was presented in [Bollt97]. The authors suggest to introduce a forbidden gap of small size at the partition zone and then neglect all trajectories which go through this gap which is possible for some maps because of an explicit characterization of the forbidden trajectories. They give also arguments (computing the topological entropy and analysing successive approximations of the grammar of the symbolic dynamics by means of a sequence of transition matrices) that for sufficiently small gap the loss of the trajectories generating the sequences is only incremental and, what it follows, such a procedure does not deteriorate the statistical properties of the sequences. From the other side, to avoid the problems connected with inaccuracy of numerical computations, we propose to consider physical realisations of CPBG. However despite avoiding the problem of computational error we face another one - accuracy of measurements.

REFERENCES

[Altsh91] Altshuler, B.L., P.A.Lee, R.A.Webb. 1991.*Mesoscopic Phenomena in Solids*, series: *Modern Problems in Condensed Matter Sciences*, vol.30, North-Holland, Amsterdam.

[Andr64] Andreyev,A.F., 1964. „Thermal conductivity of the intermediate state of superconductors." Journal of Experimental and Theoretical Physics 46: 1823-1828.

[Babo84] Babovsky, H. 1984. „Initial and boundary value problems in kinetic theory. I. The Knudsen gas, II. The Boltzmann equation." Transport Theory and Statistical Physics 13: Part I-455-474, Part II-475-498.

[Beker82] Beker, H. and F.Piper. 1982. *Cipher Systems: the Protection of Communication*. John Wiley&Sons, New York.

[Beck90] Beck, C. 1990. „Ergodic properties of a kicked damped particle." Communications in Mathematical Physics 130: 51-60.

[Bollt97] Bollt, E., Y-C.Lai and C.Grebogi. 1997. „Coding, channel capacity, and noise resistance in communicating with chaos." Physical Review Letters 79, no.19 (Nov): 3787-3790.

[Corn82] Cornfeld, L.P., S.V.Fomin and Ya.G.Sinai. 1982. *Ergodic Theory.* Springer-Verlag, Berlin.

[FIPS94]. FIPS 140-1. 1994. *Security Requirements for Cryptographic Modules.* NIST.

[Gold85] Goldstein, S., C.Kipnis and N.Ianiro. 1985. „Stationary states for a mechanical systems with stochastic boundary conditions", Journal of Statistical Physics 41: 915-938.

[Golo67] Golomb, S.W. 1967. *Shift Register Sequences*, Holden-Day, San Francisco.

[Guck83] Guckenheimer, J. and P.Holmes. 1983. *Nonlinear oscillations, dynamical systems, and bifurcations of vector fields*. Springer-Verlag, New York.

[Habu91] Habutsu, T., Y.Nishio, I.Sasase and S.Mori. 1991. „A secret key cryptosystem by iterating a chaotic map." In *Eurocrypt'91*: 127-140.

[Howe85] Howett, J.M., M.Month and S.Turner. 1985. „Nonlinear Dynamics, Aspects of Particle Accelerators." Proceedings, Sardinia, Lecture Notes in Physics, Springer-Verlag, Berlin.

[Ichi89] Ichikava, Y.H., T.Kamimura, T.Hatori and S.Y.Kim. 1989. „Stochasticity and symmetry of the standard map." Progress inTheoretic Physics. Supplement 98: 1-18.

[Kapi96] Kapitaniak, T. 1996. *Controlling Chaos, Theoretical and Practical Methods in Non-linear Dynamics*. Academic Press, London.

[Knuth81] Knuth, D.E. 1981. *The Art. of Computer Programming - Seminumerical Algorithms*, vol.2., Addison-Wesley, Reading.

[Kosj72] Kosjakin, A.A and E.A.Sandler. 1972. „Ergodic properties of some class of piecewise smooth maps on the interval." Matiematika 3: 32-40.

[Kohda97] Kohda, T. and A.Tsuneda. 1997. „Statistic of chaotic binary sequences." IEEE Transactions on Information Theory 43, no.1 (Jan): 104-112.

[Kotul97] Kotulski, Z. and J. Szczepański. 1997. „Discrete chaotic cryptography." Annalen der Physik 6, no.5(Sept): 381-394.

[Kotul99] Kotulski, Z., J.Szczepański, K.Górski, A.Paszkiewicz and A.Zugaj. 1999. „The application of discrete chaotic dynamical systems in cryptography - DCC Method." International Journal of Bifurcation and Chaos 9, no.6 (June).

[Lin84] Lin, H.B. 1984. *Chaos*, World Sc. Publ. Corp., Hong-Kong.

[Naza98] Nazarov, Y.V. 1998. „Novel circuit of Andreev reflection", Preprint cond-mat 9811155, Los Alamos.

[Ott90] Ott, E., C.Grebogi and J.A.Yorke. 1990. „Controlling chaos.", Physical Review Letters 64, no.11 (Nov): 1196-1199.

[Parl92] Parlitz, U., L.O.Chua, Lj.Kocarev, K.S.Halle and A.Shang, 1992, „Transmission of digital signals by chaotic synchronization", International Journal on Bifurcation & Chaos 2: 973-977.

[Peco90] Pecora, L.M and T.L.Caroll. 1990. „Synchronization in chaotic systems", Physics Review Letters 64, no.8(Aug): 821-824.

[Schne96] Schneier, B. 1996. *Applied Cryptography. Practical Algorithms and Source Codes in C*, John Wiley, New York.

[Schnu73] J.Schnute, M.Shinbrot. 1973. „Kinetic theory and boundary conditions for fluids." Canadian Journal of Mathematics 25: 1183.

[Szcz91] Szczepański, J. and E.Wajnryb. 1991. „Long-time behaviour of the one-particle distribution function for the Knudsen gas in a convex domain". Physical Review A 44, no.6: 3615-3621.

[Szcz95] Szczepański, J. and E.Wajnryb. 1995. „Do ergodic or chaotic properties of the reflection law imply ergodicity or chaotic behaviour of a particle's motion?" Chaos, Solitons & Fractals 5, no.1: 77-89.

[Szcz98] Szczepański, J. and Z.Kotulski. 1998. „On topologically equivalent ergodic and chaotic reflection laws leading to different types of particle's motion." Archives of Mechanics 50, no.5: 865-875.

[Szcz99] Szczepański, J., K.Górski, Z.Kotulski , A.Paszkiewicz and A.Zugaj. 1999. „Some models of chaotic motion of particles and their application to cryptography.", Archives of Mechanics 51, no.3-4(Aug.):509-528.