Open Sys. & Information Dyn. **8**: 137–146, 2001

Printed in the Netherlands

Pseudorandom Number Generators Based on Chaotic Dynamical Systems *

Janusz Szczepański

Institute of Fundamental Technological Research,
Polish Academy of Sciences, PL-00-049 Warsaw, Świętokrzyska 21
email: jszczepa@ippt.gov.pl

Zbigniew Kotulski

Institute of Fundamental Technological Research,
Polish Academy of Sciences, PL-00-049 Warsaw, Świętokrzyska 21
email: zkotulsk@ippt.gov.pl

(Received: March 14, 2001)

Abstract. Pseudorandom number generators are used in many areas of contemporary technology such as modern communication systems and engineering applications. In recent years a new approach to secure transmission of information based on the application of the theory of chaotic dynamical systems has been developed. In this paper we present a method of generating pseudorandom numbers applying discrete chaotic dynamical systems. The idea of construction of chaotic pseudorandom number generators (CPRNG) intrinsically exploits the property of extreme sensitivity of trajectories to small changes of initial conditions, since the generated bits are associated with trajectories in an appropriate way. To ensure good statistical properties of the CPRBG (which determine its quality) we assume that the dynamical systems used are also ergodic or preferably mixing. Finally, since chaotic systems often appear in realistic physical situations, we suggest a physical model of CPRNG.

1. Introduction

Pseudorandom number generators with "good" properties are frequently used in modern communication systems as well as in a variety of engineering applications. The quality in this case means: How well a given device or algorithm producing random or pseudorandom numbers imitates an ideal source of independent, uniformly distributed 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 in question.

Traditionally, extensive statistical testing was used to assess or estimate this quality. Test suites developed for this purpose may be found in [6, 11]. The American norm FIPS 140-2 [6], which is currently one of the standard benchmarks, specifies the following 4 tests on sequences of 20000 bits[1]:

* This paper has been prepared with the financial support of KBN, grant 8 T11D 020 19

[1] Possession of a good pseudorandom bit generator (PRBG) is sufficient to construct a good

1. the monobit test — the number of "1" bits in the sequence must lie within specified limits,
2. the poker test — the histogram of values of non-overlapping four bit segments must resemble the uniform distribution; in this and the previous test the χ^2 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 within 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 [16].

In the case of some classes of algorithmic pseudorandom number generators a further level of assurance has been obtained by a theoretical analysis of 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 propose a class of generators based on the theoretical foundation of chaotic and ergodic transformations.

In the last few decades, a new phenomenon called chaos [7] 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 the extreme sensitivity of trajectories to small changes of initial conditions. Such properties seem to be relevant for the construction of cryptographic algorithms. The earliest applications of chaos were based on encrypting messages by modulation of trajectories in continuous dynamical systems. These methods are strongly connected with the concept of synchronization of chaotic systems [15] and of chaos control [10]. Recently also the theory of discrete dynamical systems is applied in secure communication [8, 12]. The papers [9, 13, 14], develop the case of block ciphers, making use of multiple iterations and inverse iterations of chaotic maps.

The objective of this paper is the proposition of the method of constructing pseudorandom number generators (based on discrete chaotic dynamical systems) applicable in stream ciphers. The basic idea of construction of CPRNG exploits the property of sensitivity of the trajectories to initial conditions, which is the essence of chaos. The generated bits are associated with the behavior of trajectories. To ensure good statistical properties (which determine the quality of a generator) of the CPRNG we assume that the dynamical systems used are also ergodic or

pseudorandom number generator and it is often easier to work with bit generators.

preferably mixing. This allows us to 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 suggest some physical realizations of CPRNG.

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

2. Discrete Dynamical Systems

A discrete dynamical system is a pair (S, F), where S is the state space (usually metric space) and $F : S \to S$ is a measurable map which is the generator of the semigroup of iterations. The trajectory starting from the initial state s_0 is the sequence $(s_n)_{n=0}^{\infty}$ of elements of S obtained by iteration

$$s_{n+1} \;=\; F(s_n)\,, \qquad n = 0, 1, 2, \ldots \tag{2.1}$$

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 $DF^n(s)(v)$ be the Frechet derivative of the n-th iteration of F at s in the direction of v. Then the Lyapunov exponent is given by the limit

$$\lambda_{s,v} \;\equiv\; \lim_{n\to\infty} \frac{1}{n} \ln \|DF^n(s)(v)\|\,, \tag{2.2}$$

where $\|\cdot\|$ is the norm in the tangent space at s. Lyapunov exponents exist under some general conditions on the smoothness of F [7]. The number of different Lyapunov exponents at s is equal at most to the dimension of the tangent space.

Among many existing formal definitions of chaos [4] the most exploited in the literature is the one using the concept of Lyapunov exponents. We say that a nonlinear dynamical system is chaotic in some region if for almost all points s (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 points, after several 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 $x \in R$, $\lambda_x > 0$ then

$$\begin{gathered} \forall\, \varepsilon > 0 \quad \exists\, n_1, n_2 \quad \exists\, U_{n_1,n_2} \ni x \quad \forall\, n_1 \le n \le n_2 \quad \forall\, z_1, z_2 \in U_{n_1,n_2} \\ e^{(\lambda_x - \varepsilon)n} |z_1 - z_2| \;<\; |\psi^n(z_1) - \psi^n(z_2)| \;<\; e^{(\lambda_x + \varepsilon)n} |z_1 - z_2|\,. \end{gathered} \tag{2.3}$$

In (2.3), U_{n_1,n_2} is an open neighborhood of x. It is essential for practical construction of secure information transmission to select the appropriate natural numbers n_1 and n_2 to guarantee sufficient accuracy of calculations.

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

$$\forall\, A \in \sigma(S)\,, \qquad \mu(A) \;=\; \mu(F^{-1}(A))\,, \tag{2.4}$$

where $\sigma(S)$ is the σ-algebra of measurable subsets of S.

Constructing a cryptographic algorithm, we consider dynamical systems for which some invariant measure μ exists and is equivalent to the Lebesgue measure with its density function $g(s)$ satisfying, for positive constants g_1, g_2,

$$0 \;<\; g_1 \;\leq\; g(s) \;\leq\; g_2\,,$$

where $\forall\; A \in \sigma(S)$, $\mu(A) = \int_A g(s)ds$). 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 an appropriate choice of the map F.

We say that a dynamical system (S, F) is ergodic [5] if and only if it has only trivial invariant sets, i.e., if and only if either $\mu(B) = 0$ or $\mu(S\backslash B) = 0$, 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 a trajectory starts from any point $s_0 \in S$, it never settles 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. (In the case of smaller disjoint parts any "brute force" attack is restricted to one part of the partition which significantly reduces its numerical complexity).

The next important characteristic of trajectories (stronger than ergodicity) is the mixing property. A dynamical system is called mixing [5] if the following condition is satisfied (for $\mu(S) = 1$):

$$\lim_{n\to\infty} \frac{\mu(F^{-n}(A) \cap B)}{\mu(B)} \;=\; \frac{\mu(A)}{\mu(S)}\,. \tag{2.5}$$

From this formula we can see that the part of B which after n iterations of F is contained in A is asymptotically proportional to the volume (in the sense of the measure μ) of A in S.

Formula (2.5) gives an asymptotic condition for the spreading of B over the whole space S under iteration. It is also important to specify the speed of such phenomenon. In the case of K-systems [5] the convergence is exponential,

$$|\mu(F^{-n}(A) \cap B) - \mu(A)\mu(B)| \;\leq\; e^{-qn}\,, \tag{2.6}$$

for all n satisfying: $n_0 \;\leq\; n$ (n_0 is some natural number) and some fixed $q > 0$ depending on F.

Mixing property means that the trajectories of the system have a property of stochasticity. If we assume the measure μ to be probabilistic then the iterations of F make each set A (asymptotically) statistically independent from B. In other words, if we start our trajectory from a vicinity of $s_0 \in S$ then after sufficiently many iterations we can reach any region of 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" in the sense that studying finite-dimensional distributions in the state space we cannot distinguish whether the system is chaotic or stochastic. Therefore a chaotic dynamical system seems to be a good candidate for the source of random numbers (bits).

3. Construction of the Chaotic Generator

In this section, we propose the application of discrete dynamical systems for construction of chaotic pseudorandom bit generators (CPRBG). To ensure the 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 as follows. Let us assume that we have some dynamical system $F : S \to S$, where S is the state space and by μ we denote a normalized invariant measure of the system. The central point of construction is to divide the state space in an 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 observe 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 $b_n(s)$ of the generated sequence is equal to "0" if $s_n \in S_0$, and is equal to "1" otherwise. This way, we obtain the infinite sequence of bits $G(s)$. Thus, we obtain the map

$$G : S' \to \prod_{i=1}^{\infty} \{0,1\}\,, \tag{3.1}$$

such that

$$G(s) = \{b_i(s)\}_{i=1,2,\ldots} = \{b_1(s), b_2(s), \ldots\}\,, \tag{3.2}$$

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

4. Properties of CPRBG

To verify the correctness of the presented construction we should prove 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 (3.1)–(3.2) we have

THEOREM 1. *For each $s \in S$ the following holds true:*

$$\mu(G^{-1}(\{b_i(s)\})) = 0\,. \tag{4.1}$$

Proof. Fix $s \in S$. Consider the sequence of bits

$$G(s) = \Big\{ b_1(s), b_2(s), b_3(s), \ldots, b_n(s), \ldots \Big\}. \tag{4.2}$$

To simplify the notation we write further b_i instead of $b_i(s)$ and we introduce

$$S_{b_i} \;=\; S_0 \quad \text{for} \quad b_i \;=\; 0 \tag{4.3}$$

and

$$S_{b_i} \;=\; S_1 \quad \text{for} \quad b_i \;=\; 1\,. \tag{4.4}$$

Define the sets

$$\begin{aligned} A_{b_1} \;&:=\; F^{-1}(S_{b_1})\,, \\ A_{b_1 b_2} \;&:=\; F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2})\,, \end{aligned}$$

and, generally, $A_{b_1 b_2 \ldots b_n} \subset S$, $n = 3, 4, 5, \ldots$,

$$A_{b_1 b_2 \ldots b_n} \;:=\; F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2}) \cap \ldots \cap F^{-n}(S_{b_n})\,. \tag{4.5}$$

Observe that for every $n = 1, 2, \ldots$, $A_{b_1 b_2 \ldots b_n}$ is the set of all seeds z such that the first n initial bits of $G(z)$ are $(b_1, b_2, b_3, \ldots, b_n)$. More precisely,

$$z \in A_{b_1 b_2 \ldots b_n} \implies b_i(z) \;=\; b_i(s), \qquad \text{for} \quad i = 1, 2, \ldots, n\,. \tag{4.6}$$

This follows from the fact that for $i = 1, 2, \ldots, n$

$$F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2}) \cap \ldots \cap F^{-n}(S_{b_n}) \;\subseteq\; F^{-i}(S_{b_i})\,, \tag{4.7}$$

and, consequently:

$$F^i(z) \in F^i\Big(F^{-1}(S_{b_1}) \cap \ldots \cap F^{-n}(S_{b_n})\Big) \;\subseteq\; F^i(F^{-i}(S_{b_i})) \;=\; S_{b_i} \;\equiv\; S_{b_i(s)}\,, \tag{4.8}$$

which proves (4.6).

By the basic property of measure we have

$$\mu\Big(F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2}) \cap \ldots \cap F^{-n}(S_{b_n})\Big) \;\leq\; \mu(F^{-1}(S_{b_1}) \;\cap\; F^{-n}(S_{b_n}))\,. \tag{4.9}$$

Now we apply the mixing property (2.5) to the two sets

$$F^{-1}(S_{b_1}) \quad \text{and} \quad S_{b_n} \tag{4.10}$$

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

$$\mu\Big(F^{-1}(S_{b_1}) \cap F^{-n_1}(S_{b_{n_1}})\Big) \;\leq\; \mu\Big(F^{-1}(S_{b_1})\Big)\mu(S_{b_{n_1}}) + \varepsilon\,. \tag{4.11}$$

Since μ is invariant, from (4.9) and (4.11) we obtain:

$$\mu\Big(F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2}) \cap \ldots \cap F^{-n_1}(S_{b_{n_1}})\Big) \;\leq\; \mu(S_{b_1})\mu(S_{b_{n_1}}) + \varepsilon\,. \tag{4.12}$$

Applying the mixing property (2.5) to the sets $A = S_{b_{n_2}}$, where

$$S_{b_{n_2}} = S_0 \quad \text{or} \quad S_{b_{n_2}} = S_1 \tag{4.13}$$

for a certain $n_2 > n_1$, and

$$B \;=\; F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2}) \cap \ldots \cap F^{-n_1}(S_{b_{n_1}})\,, \tag{4.14}$$

and using (4.12) we have that if n_2 is sufficiently large then

$$\begin{aligned}
&\mu\Big(F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2}) \cap \ldots \cap F^{-n_1}(S_{b_{n_1}}) \cap \ldots \cap F^{-n_2}(S_{b_{n_2}})\Big) \\
&\qquad \le\; \mu\Big(F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2}) \cap \ldots \cap F^{-n_1}(S_{b_{n_1}}) \cap F^{-n_2}(S_{b_{n_2}})\Big) \\
&\qquad \le\; \mu\Big(F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2}) \cap \ldots \cap F^{-n_1}(S_{b_{n_1}})\Big)\mu\Big(F^{-n_2}(S_{b_{n_2}})\Big) + \varepsilon \\
&\qquad \le\; \Big[\mu\Big(F^{-1}(S_{b_1})\Big)\mu\Big(F^{-n_1}(S_{b_{n_1}})\Big) + \varepsilon\Big]\mu\Big(F^{-n_2}(S_{b_{n_2}})\Big) + \varepsilon\,.
\end{aligned} \tag{4.15}$$

By the invariance property of the measure μ and the symmetry condition $\mu(S_0) = \mu(S_1) = 1/2$, we obtain from (4.15) the following inequality:

$$\mu\Big(F^{-1}(S_{b_1}) \cap F^{-2}(S_{b_2}) \cap \ldots \cap F^{-n_1}(S_{b_{n_1}}) \cap \ldots \cap F^{-n_2}(S_{b_{n_2}})\Big) \;\le\; \frac{1}{2}\Big(\frac{1}{2}\cdot\frac{1}{2} + \varepsilon\Big) + \varepsilon\,. \tag{4.16}$$

In general, using the complete induction property, we can find a sequence $\{n_1, \ldots, n_p\}$ for any p such that

$$\begin{aligned}
&\mu(A_{b_1 b_2 \ldots b_{n_1} \ldots b_{n_2} \ldots b_{n_p}}) \;:= \\
&\quad :=\; \mu\Big(F^{-1}(S_{b_1}) \cap \ldots \cap F^{-n_1}(S_{b_{n_1}}) \cap \ldots \cap F^{-n_2}(S_{b_{n_2}}) \cap \ldots \cap F^{-n_p}(S_{b_{n_p}})\Big) \\
&\qquad \le\; \Big\{\Big[\Big(\mu(S_{b_1})\mu(S_{b_{n_1}}) + \varepsilon\Big)\mu(S_{b_{n_2}}) + \varepsilon \ldots\Big]\mu(S_{b_{n_p}}) + \varepsilon\Big\} + \varepsilon \\
&\qquad \le\; \Big\{\Big[\Big(\frac{1}{2}\cdot\frac{1}{2} + \varepsilon\Big)\frac{1}{2} + \varepsilon \ldots\Big]\frac{1}{2} + \varepsilon\Big\} + \varepsilon\,.
\end{aligned} \tag{4.17}$$

We see that the right hand side of the above inequality is equal to the value of the n_p-th iteration of the function $h(x) = x/2 + \varepsilon$ at $x = 1/2$. For n_p sufficiently large, we have

$$h^{n_p}\Big(\frac{1}{2}\Big) \;<\; 3\,\varepsilon\,. \tag{4.18}$$

Moreover, $A_{b_1 b_2 \ldots b_n} \subseteq A_{b_1 b_2 \ldots b_m}$ for every $n \le m$ and

$$\mu(A_{b_1 b_2 \ldots b_n}) \;\le\; \mu(A_{b_1 b_2 \ldots b_m})\,. \tag{4.19}$$

This means that the sequence of numbers $\mu(A_{b_1 b_2 \ldots b_n})$, $n = 1, 2, \ldots$ is monotonic and, since $\varepsilon > 0$ can be arbitrarily small, we deduce from (4.17)–(4.18) that it contains a subsequence converging to zero. Thus,

$$\lim_{n\to\infty} \mu(A_{b_1 b_2 \ldots b_n}) \;=\; 0\,, \tag{4.20}$$

which concludes the proof of Theorem 1. □

In practice, for the introduced partition of the state space S, due to chaotic property, any two different seeds (initial conditions), independent of how close they are, lead to completely different sequences of bits. This property is very important in applications.

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

By ergodicity we obtain that the expected number of "0" bits in the generated sequence is equal to the expected number of "1" bits. To be more precise, we can use the Birkhoff-Khinchin Ergodic Theorem [5], which applied to our system gives:

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\chi_{S_0}(F^i(s)) \;=\; \int_S \chi_{S_0}\,d\mu \;=\; \mu(S_0)\,, \tag{4.21}$$

where χ_{S_0} is the indicator function of the set S_0 and $s \in S'$ ($\mu(S\backslash S') = 0$). Since by our assumption $\mu(S_0) = 1/2$ 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 ergodic map with itself is also ergodic, we have that any subsequence $(b_{kn})_{n=1,2,\ldots}$ has the above property, too.)

The mixing property, defined by the condition (2.5), means that any measurable set $A \subset S$ will be μ-uniformly distributed over the whole state space S under iteration. We use this property to prove the theorem which states that the bits generated by CPRBG are asymptotically independent.

THEOREM 2. *For $n = 1, 2, \ldots$, the bits B_n, B_{n+k} (considered as random variables) generated by a given mixing dynamical system (S, F) are asymptotically independent as k increases.*

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:

$$Y_k^n(s) \;:=\; \chi_{S_0}(H_k^n(s)) \;=\; \chi_{S_0}\Big((F^k)^n(s)\Big)\,, \tag{4.22}$$

acting on the probabilistic space $\{S', \sigma(S'), \mu\}$, 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 CPRBG based on the dynamical system (S, F).

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:

$$\sigma_k^n \;=\; \Big\{\emptyset, S', F^{-nk}(S_0'), F^{-nk}(S_1')\Big\} \tag{4.23}$$

and

$$\sigma_k^{n+1} \;=\; \left\{\emptyset, S', F^{-(n+1)k}(S'_0), F^{-(n+1)k}(S'_1)\right\}. \tag{4.24}$$

When k is sufficiently large, we have:

$$\begin{aligned}\mu\Big(F^{-(n+1)k}(S'_\alpha)\cap F^{-nk}(S'_\beta)\Big) &= \mu\Big(F^{-k}(F^{-nk}(S'_\alpha))\cap F^{-nk}(S'_\beta)\Big)\\ &\approx \mu\Big(F^{-nk}(S'_\alpha)\Big)\mu\Big(F^{-nk}(S'_\beta)\Big),\end{aligned} \tag{4.25}$$

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

The last relation follows from the mixing property (2.5) and the approximation becomes more accurate as k increases. The relation (4.25) is in fact the definition of independence of the random variables $B_n := Y_k^n$ and $B_{n+k} := Y_k^{n+1}$, which gives the conclusion of Theorem 2. □

Utilizing the result of Theorem 2, we take for the construction of CPRBG the modified dynamical system

$$(S', H_k^1) \;:=\; (S', F^k), \tag{4.26}$$

for sufficiently large k, and we obtain sequences of statistically independent random bits.

5. Final Remarks

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

In the process of generation of 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 the sets S_0 and S_1, then the numerical error can make a "0" bit generated in one computer become "1" bit in another (or vice versa). The idea of how to prevent this inconvenience was presented in [3]. 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 also give arguments (computing topological entropy and analyzing successive approximations of the grammar of symbolic dynamics by means of a sequence of transition matrices) that for a sufficiently small gap the loss of trajectories generating the sequences is negligible and, therefore, such a procedure does not deteriorate the statistical properties of the sequences. On the other hand, to avoid problems connected with inaccuracy of numerical computations, we suggest to consider physical models of CPRBG. There are many chaotic dynamical systems

in real life. It could be promising to construct physical systems realizing our cryptographic algorithms.

An interesting example is the application of non-classical reflection law models, originating from the kinetic theory of dilute gases, which is the source of the concept of chaos and ergodicity. The theory of non-classical reflection laws found its place in the literature [1, 17, 18, 19]. The models describe the motion of a free particle in a bounded domain. To establish the model, one must select a domain with a certain boundary shape and define the reflection law. The generation is the observation of the evolution of a particle starting from an initial state, playing the role of the seed. The sequence of bits is generated by taking the n-th bit equal to "0" if the state of the particle at the moment of the n-th reflection is observed in some subset of the state space, and "1" otherwise. In models of such kind chaos property of the reflection law is transferred to the dynamical system describing the motion of a particle [2, 14]. Thus, the security of the cryptosystem based on unpredictability of the location of a moving particle is assured by its chaotic behavior. Although physical realization of the CPRBG allows us to avoid the problem of computational error, we face another one — the accuracy of physical measurements.

Bibliography

[1] H. Babovsky, Transport Theory and Statistical Physics **13**, Part I 455, Part II 475 (1984).

[2] C. Beck, Comm. Math. Phys. **130**, 51 (1990).

[3] E. Bollt, Y-C. Lai, and C. Grebogi, Phys. Rev. Lett. **79**, 3787 (1997).

[4] R. Brown and L. O.Chua, International Journal of Bifurcation and Chaos **6**, 219 (1996).

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

[6] FIPS 140-2, *Security Requirements for Cryptographic Modules*, NIST, 2000.

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

[8] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, Proceedings EUROCRYPT'91, 127 (1991).

[9] G. Jakimoski and L. Kocarev, IEEE Transactions on Circuits and Systems I-Fundamental Theory and Applications **48**, 163 (2001).

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

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

[12] T. Kohda and A. Tsuneda, IEEE Transactions on Information Theory **43**, 104 (1997).

[13] Z. Kotulski and J. Szczepański, Ann. Phys. **6**, 381 (1997).

[14] Z. Kotulski, J. Szczepański, K. Górski, A. Paszkiewicz, and A. Zugaj, International Journal of Bifurcation and Chaos **9**, 1121 (1999)

[15] U. Parlitz, L.O. Chua, L. Kocarev, K. S. Halle, and A. Shang, International Journal on Bifurcation and Chaos **2**, 973 (1992).

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

[17] J. Schnute and M. Shinbrot, Canadian Journal of Mathematics **25**, 1183 (1973).

[18] J. Szczepański and E. Wajnryb, Chaos, Solitons and Fractals **5**, 77 (1995).

[19] J. Szczepański and Z. Kotulski, Archives of Mechanics **50**, 865 (1998).