ON CONSTRUCTIVE APPROACH TO CHAOTIC PSEUDORANDOM NUMBER GENERATORS

Zbigniew Kotulski, Janusz Szczepański

Polish Academy of Sciences, Institute of Fundamental Technological Research

Świętokrzyska 21, 00-049 Warsaw, Poland

E-mail: zkotulsk@ippt.gov.pl.

Karol Górski, Anna Górska, Andrzej Paszkiewicz

Warsaw University of Technology, Institute of Telecommunications

Nowowiejska 15/19, 00-665 Warsaw, Poland

E-mail: anpa@tele.pw.edu.pl.

KEYWORDS

Pseudorandom number generators, stream ciphers, dynamical systems, chaos, ergodicity, solvable chaotic systems, statistical tests.

ABSTRACT[1]

Among pseudorandom number generators widely used in engineering applications, Chaotic Pseudorandom Number Generators (CPRNG) have particularly attractive properties which guarantee the uniqueness of the generated sequences for any chosen seed and the independence of the generated numbers along the obtained trajectory (the sequence). These properties can be rigorously mathematically proved for a wide class of chaotic dynamical systems. The appropriate theorems can be found in the previous paper of the authors (Szczepański et al.1999a).

In this paper we develop the results obtained in (Szczepański et al.1999a) and present a class of generators based on the so-called solvable (constructible) chaotic dynamical systems. In this case the elements of the chaotic sequence can be represented in an iterative way and, alternatively, as certain functions of the argument *n*. We study the effectiveness of the practical application of such systems for generation of sequences of pseudorandom numbers and investigate the properties of the obtained data to confirm the validity of the proposed algorithm for cryptographic purposes.

[1] This work has been partially supported by grant no. 8 T11D 020 19 of the Polish State Committee for Scientific Research.

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. Test suites developed for this purpose may be found in (Knuth 1981; Beker and Piper 1982; FIPS 140-1). For example, FIPS 140-1 specifies the following 4 tests on sequences of 20000 bits. (Possession of a good pseudorandom bit generator (PRBG) is sufficient to construct a good pseudorandom number generator and it is often easier to work with bit generators.):

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 resemble 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 (based on Walsh or Fourier transforms), entropy tests and tests of linear, maximal order or sequence complexity profiles (Schneier 1996).

In the case of pseudorandom number generators, some a priori conditions for their acceptance were formulated by Golomb (Golomb 1967). 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.

The above testing procedures are certain schedules of investigation of general properties of bit sequences like independence and equidistribution. More procedures and particular tests can be found in (Knuth 1981; Wieczorkowski and Zieliński 1997).

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.

In the last few decades, a new phenomenon called chaos (Lin 1984) 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 prove to be non-distinguishable from truly random trajectories, see (Taylor 1993; 1996). The essential property of such systems is extreme sensitivity of the trajectories to small changes to initial conditions (Lin 1984). Such properties seem to be relevant during construction of cryptographic algorithms. Therefore the theory of chaotic dynamical systems is recently extensively applied for construction of cryptographic systems (both block ciphers (Habutsu et al. 1991) and stream ciphers (Kohda and Tsuneda 1997)). 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 (Parlitz et al. 1992; Pecora and Caroll 1990) and controlling chaos (Kapitaniak 1996; Ott et al. 1990). Another idea is to make use of discrete dynamical systems, see (Saber 2000), to construct secure cryptosystems (Kotulski and Szczepański 1997; Kotulski et al. 1999). It was developed for 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.

BASIC DEFINITIONS AND FACTS

The fundamental term in our approach is the dynamical system. 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* which is 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 possibility of application of discrete dynamical systems for generation of qualified random

numbers is conditioned by chaos which, 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), comp. (Szczepański et al. 1999a). The intuitive concept of chaos has been described in various ways; in (Brown and Chua 1996) the authors discuss a number of such properties of trajectories of dynamical systems and their mutual relations. They also give counterexamples for the properties considered in past to define chaos (e.g., the Poincare map generated by a trajectory of a dynamical system constitutes a strange attractor) but, in fact, being insufficient. Here we list several sufficient conditions satisfied by a dynamical system to guarantee chaos[2]:

- The system has periodic orbits of any order $k = 1,2,...$ and it exists an uncountable subset $W \subset S$ (containing no periodic points) such that: any two different trajectories starting from it never overlap but meet (in a certain sense) infinitely many times and every trajectory starting from this set never converge to a periodic trajectory (Li and Yorke 1975).
- The system has positive topological entropy (Katok 1980).
- The spectral density of trajectories (considered as a time-series) has a component that is absolutely continuous with respect to Lebesgue measure (Bergé et al. 1984).
- The trajectories of the system satisfy certain statistical properties (Shilnikov 1984).
- The trajectories of the system have positive algorithmic complexity (Ford 1986).
- The system has a Smale horseshoe (de Almeida 1988).
- The system has positive Kolmogorov entropy (Schuster 1988).
- The system has a dense set of periodic orbits, is topologically transitive, and has sensitivity to initial conditions (Devaney 1989).
- The system has sensitivity to initial conditions and is topologically transitive (Wiggins 1992).
- The system has a positive Lyapunov exponent (Gulick 1992).

[2] These and other related properties of chaotic dynamical systems are explained in details in (Brown and Chua 1996) or in papers cited therein.

The most popular (and the most convenient in applications) definition of chaos is closely related to the concept of Lyapunov exponents. Now we remind the fundamental definitions needed to formulate the problem.

Assume, $s \in S$, v is 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. The Lyapunov exponent is defined as:

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

where $\| \ \|$ is the norm in the tangent space at point s. The Lyapunov exponents exist under some general conditions concerning smoothness of F (Guckenheimer and Holmes 1983). The number of different Lyapunov exponents at s is at most equal to the dimension of the tangent space.

Let $\sigma(S)$ be the σ–algebra of measurable subsets of S. The measure μ on $\sigma(S)$, $\mu(S) < \infty$, is F-invariant if it satisfies the condition:

$$\forall A \in \sigma(S), \quad \mu(A) = \mu\left(F^{-1}(A)\right). \qquad (3)$$

We say that the dynamical system (S,F) 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 at least one positive Lyapunov exponent. If the system has at least two positive Lyapunov exponents it is called *hyperchaotic,* see, e.g., (Yang et al. 2000).

In our considerations, we choose such a map F that for the dynamical system (S,F) some invariant measure μ, equivalent to the Lebesgue measure, exists and its density function $g(s)$ satisfies: $0 < g_1 \le g(s) \le g_2$ (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.

We say that a dynamical system (S,F) is ergodic (Cornfeld et al. 1982) 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. Inversely, knowing the final state of the system, we can never identify the region (smaller than *S*) where the trajectory started.

The dynamical system (S,F) is mixing (Cornfeld et al. 1982) if for each $A,B \in \sigma(S)$,

$$\lim_{n\to\infty} \mu\left(F^{-n}(A)\cap B\right) = \mu(A)\mu(B). \qquad (4)$$

In (4) $F^{-n}(A)$ is the pre-image of the set *A* under the *n*-th iteration of F. If $\mu(S)=1$ (the measure μ is probabilistic), then formula (4) is equivalent to

$$\lim_{n\to\infty} \frac{\mu\left(F^{-n}(A)\cap B\right)}{\mu(B)} = \frac{\mu(A)}{\mu(S)}. \qquad (5)$$

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*, see (Szczepański et al. 1999a). Moreover, formula (5) shows that iterations of F make each set *A* (asymptotically) statistically independent from *B*. This means that the trajectory starting at a fixed point $s_0 \in S$, after iterations, reaches any region of the space *S* with the same probability. Inversely, for a fixed final state s_n and sufficiently large *n*, any initial state s_0 is μ-equiprobable.

THE CHAOTIC PSEUDORANDOM NUMBER GENERATOR

The properties of dynamical systems like chaos, ergodicity, and mixing make it to be a good candidate for construction of a random numbers generator. In (Szczepański et al. 1999a) we presented such a construction of chaotic pseudorandom bit generator (CPRBG). Now, we remind briefly our reasoning to make a basis for further considerations.

Let us assume that we have the dynamical system (S,F) with a normalized invariant measure μ. We divide the state space S 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 of CPRBG, we take 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 initiated at s, i.e., the sequence $s_n := F^n(s)$ of iterations of the map F. The *n*-th bit b_n of the generated sequence is equal to "0" if $F^n(s) \in S_0$ and is equal to "1" otherwise. This way, we obtain the infinite sequence of bits $G(s)$. Thus, we obtain the map:

$$G : S' \to \prod_{i=1}^{\infty} \{0,1\}, \qquad (6)$$

such that

$$G(s) = \{b_i(s)\}_{i=1,2,\ldots} = \{b_1(s), b_2(s), \ldots\}, \qquad (7)$$

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

It can be shown that, under the conditions of chaos, ergodicity, and mixing (stronger than ergodicity), the CPRBG has the fundamental properties of generators: unique dependence of the sequence from the seed, equiprobable occurrence of “0” and “1”, and asymptotic statistical independence of bits (see (Szczepański et al. 1999a)).

Theorem 1

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

$$\mu\left(G^{-1}(\{b_i(s)\})\right) = 0. \qquad (8)$$

Theorem 1 says that if we take two different seeds in the generator then, with probability one, we obtain two different sequences of bits. In practice, due to chaos, 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.

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 (Cornfeld et al. 1982) which, for our system, can be written as:

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} \chi_{S_0}\left(F^i(s)\right) = \int_S \chi_{S_0}\, d\mu = \mu(S_0), \qquad (9)$$

where χ_{S_0} is the indicator function of the set 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 $1/2$.

The same is true for any subsequence $(b_{kn})_{n=1,2,...}$ of the original sequence $G(s) = \{b_i(s)\}_{i=1,2,...}$.
The consequence of the mixing property (4) is the asymptotic independence of bits.

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

Then, taking for construction of CPRBG the modified dynamical system $(S', H_k^1) := (S', F^k)$, for sufficiently large k, we obtain sequences of statistically independent random bits. The other, more advanced statistical properties of the CPRBG (see Introduction) depend on a certain form of the map F and of the partition S_0, S_1, and must be verified by statistical tests.
The final problem is connected with practical application of the algorithm: one must ensure the complete repeatability of the generator's algorithm, what is connected with numerical accuracy of computer calculations. In CPRBG, 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" generated in one computer become "1" in another (or vice versa). The idea of how to prevent this inconvenience is to introduce a forbidden gap (see (Bollt et al. 1997)) of small size at the partition zone and, then, neglect all trajectories that go through this gap. Such a procedure does not deteriorate the statistical properties of the sequences.
One of the possibilities of avoiding the problems connected with inaccuracy of numerical computations is a physical realisation of CPRBG, proposed in (Szczepański et al. 1999a). In this paper we present another possibility of solving (at least partially) this problem.

EXACTLY CONSTRUCTIBLE CHAOTIC SYSTEMS

To explain the idea let us start from the two known examples of chaotic maps. Consider the logistic map generating the chaotic and mixing sequence, see (Helleman 1980),

$$X_{n+1} = 4X_n(1 - X_n). \tag{10}$$

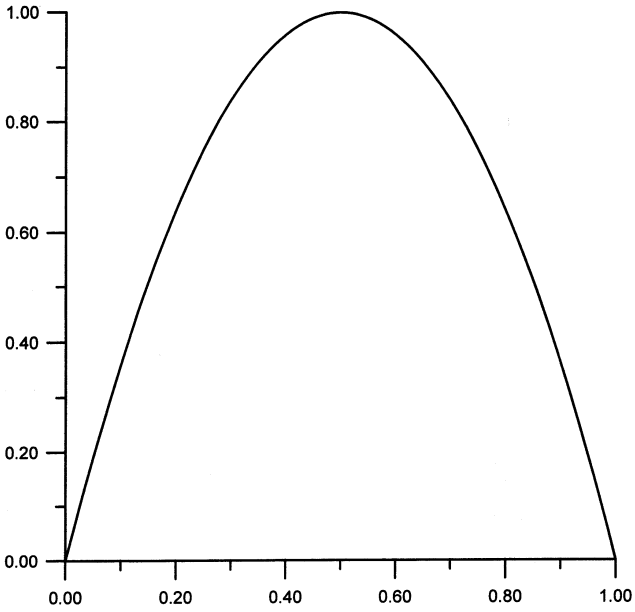

Fig. 1. The map defined by formula (10).

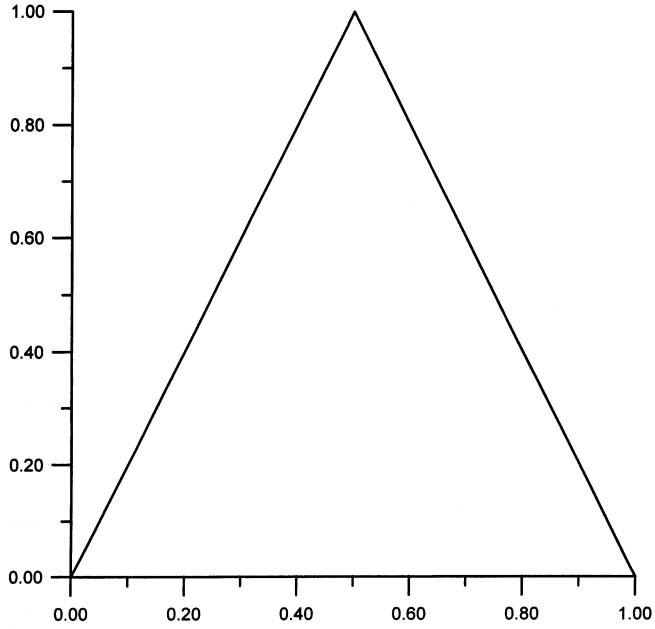

Fig. 2. The map defined by formula (12).

Its solution (the exact expression for the n-th element of the sequence) has the analytic form

$$X_n = \sin^2(2^n \arcsin\sqrt{X_0}). \tag{11}$$

Analogously, the chaotic dynamical system governed by the baker's transformation, see (Helleman 1980),

$$X_{n+1} = \begin{cases} 2X_n & 0 \le X_n < \frac{1}{2} \\ 2(1 - X_n) & \frac{1}{2} \le X_n \le 1 \end{cases}, \tag{12}$$

has the analytic exact form

$$X_n = \frac{1}{\pi}\arccos(\cos 2^n \pi X_0). \qquad (13)$$

The solutions (11) and (13) of the dynamical systems lead directly to a number of new solvable chaotic dynamical systems. For example, a natural generalization of the expression (11) is

$$X_n = \sin^2\left((k)^n \arcsin\sqrt{X_0}\right), \qquad (14)$$

for $k = 2,4,...$, and $X_i \in [0,1]$, and

$$X_n = \sin\left(k^n \arcsin X_0\right), \qquad (15)$$

for $k = 3,5,....$, and $X_i \in [-1,1]$.

The expression (13) for k greater than 2 transfers to

$$X_n = \frac{1}{\pi}\arccos\left(\cos k^n \pi X_0\right). \qquad (16)$$

For example, writing explicitly, we obtain the map and the exact solution (we keep in mind all the trigonometric identities to obtain the map expressions):

for formula (14), $k = 4$:

$$X_{n+1} = 16X_n(1-X_n)(1-2X_n)^2, \qquad (17)$$

$$X_n = \sin^2\left(4^n \arcsin\sqrt{X_0}\right); \qquad (18)$$

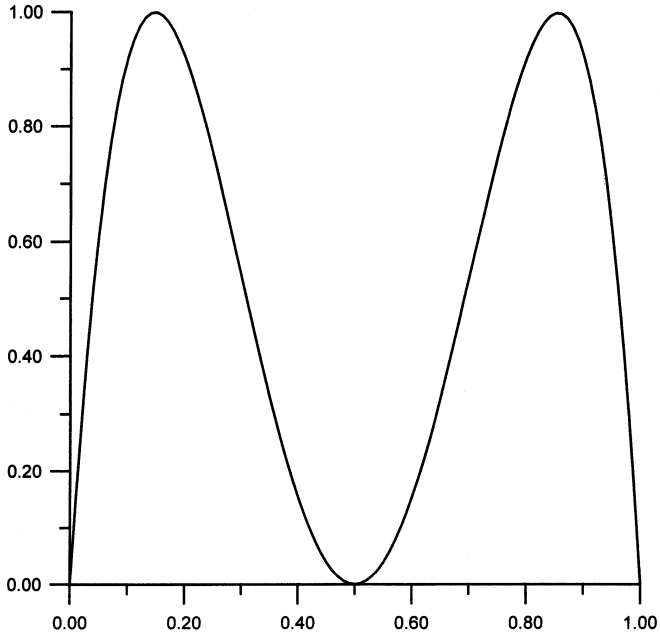

Fig. 3. The map defined by formula (17).

for formula (15), $k = 3$:

$$X_{n+1} = X_n(3-4X_n^2), \qquad (19)$$

$$X_n = \sin^2\left(3^n \arcsin X_0\right); \qquad (20)$$

for formula (15), $k = 5$

$$X_{n+1} = X_n(5-20X_n^2+16X_n^4), \qquad (21)$$

$$X_n = \sin^2\left(5^n \arcsin X_0\right); \qquad (22)$$

etc.

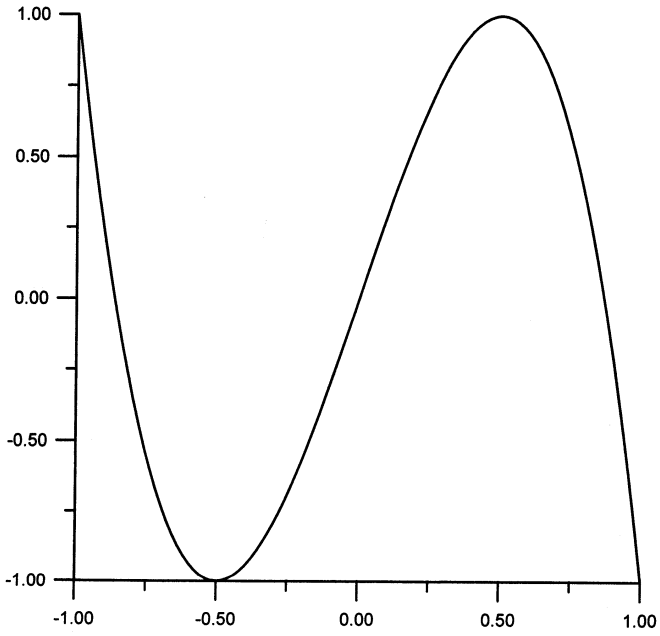

Fig. 4. The map defined by formula (19).

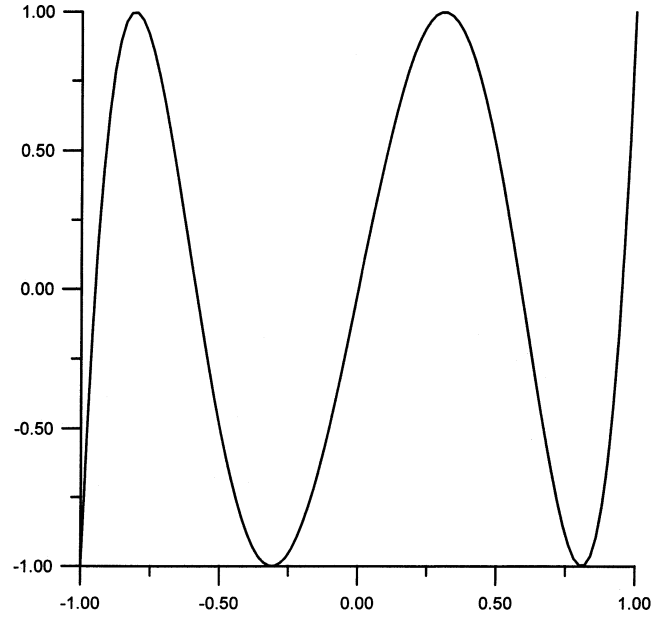

Fig. 5. The map defined by formula (21).

Analogously, for the general exact solution of the form (16) we obtain the explicit expressions:

for $k = 3$:

$$X_{n+1} = \begin{cases} 3X_n, & 0 \le X_n < \frac{1}{3}, \\ 2-3X_n, & \frac{1}{3} \le X_n < \frac{2}{3}, \\ -2+3X_n, & \frac{2}{3} \le X_n \le 1, \end{cases} \qquad (23)$$

$$X_n = \frac{1}{\pi}\arccos\left(\cos 3^n \pi X_0\right); \qquad (24)$$

for $k = 4$

$$X_{n+1} = \begin{cases} 4X_n, & 0 \le X_n < \frac{1}{4}, \\ 2(1-2X_n), & \frac{1}{4} \le X_n < \frac{2}{4}, \\ 2(2X_n - 1), & \frac{2}{4} \le X_n < \frac{3}{4}, \\ 4(1-X_n), & \frac{3}{4} \le X_n \le 1, \end{cases} \qquad (25)$$

$$X_n = \frac{1}{\pi}\arccos\left(\cos 4^n \pi X_0\right); \qquad (26)$$

etc.

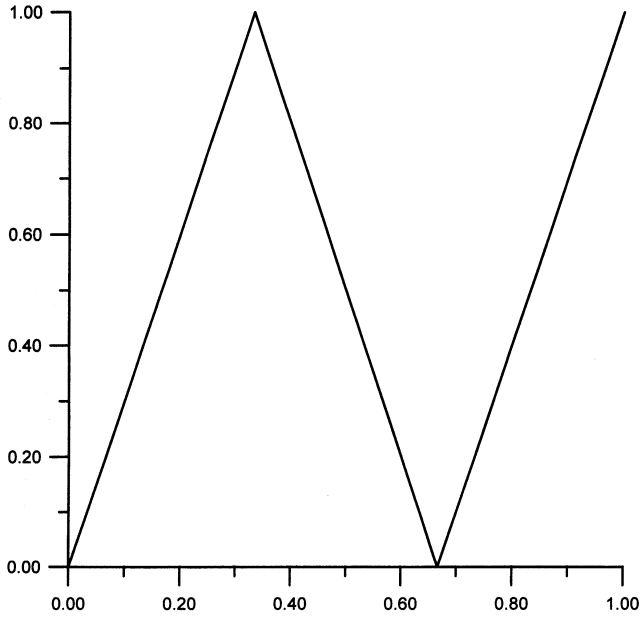

Fig. 6. The map defined by formula (23).

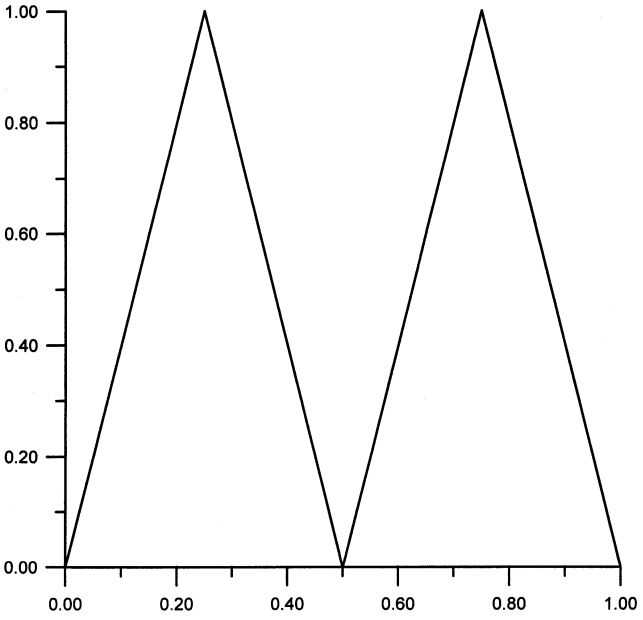

Fig 7. The map defined by formula (25).

More explicit expressions of such and similar type can be found in (Katsuda and Fukuda 1985).

The dynamical systems presented above are defined by iteration of maps. However, the systems are of such a specific type that the *n*-th term can be expressed as a combination of elementary functions. Therefore they are called the exactly solvable dynamical systems. In dedicated papers and monographs one can find a number exactly solvable chaotic maps; all the known solutions can be represented the following general form:

$$X_n = \Psi(\theta T \kappa^n), \qquad (27)$$

where:

$\Psi(t)$ is a periodic function (trigonometric, elliptic, hypoelliptic, Weirstrass, etc.),

κ is an integer number,

T is the period of the function $\Psi(t)$,

$X_0 = \Psi(\theta T)$ is the initial condition of the chaotic system (θ is a real parameter defining this condition).

The Lyapunov exponent of such a system can be calculated and it is equal to

$$\lambda = \ln \kappa. \qquad (28)$$

The exactly solvable chaotic dynamical systems enable us to increase the accuracy and the speed of calculations. Instead of iterating the map, one can calculate the value of the element using the exact expression, avoiding the summation of numerical errors during iterations. This procedure is especially effective when we take every *k*-th element of the realization of the dynamical system, avoiding this way $k-1$ iterations of the map.

The disadvantage of such a generator (no the level of generation of the realization elements, not the generation of the bit sequence) is the one-step predictability of the system. Simply, the first return map (X_n, X_{n+1}) coincides with the plot of the (real) function $y = F(x)$, where $F(x)$ is the map of the real dynamical system[3]. The remedy for this disadvantage is application of non-solvable but some way constructible chaotic dynamical systems.

To introduce the concept of constructible dynamical systems consider the map of the form

$$X_{n+1} = \sin^2(z \arcsin\sqrt{X_n}), \qquad (29)$$

where z is an integer parameter. The solution is of equation (29) is the solvable dynamical system

$$X_n = \sin^2(\pi\theta z^n); \qquad (30)$$

its Lyapunov exponent is $\lambda = \ln z$ and the system is

[3] For the examples of the exactly solovable dynamical systems considered in this paper, the state space *S* is the interval [0,1] or [-1,1].

chaotic for $z > 1$. Certainly, the function (29) is one-step predictable.

Consider now the sequence of the form (30). If the parameter *z* in (30) is fractional then the dynamical system generated is chaotic but multivalued; it cannot be expressed in the form

$$X_{n+1} = F(X_n), \tag{31}$$

see (González and Pino 2000). In particular, when z in (30) is expressed as the fraction

$$z = \frac{p}{q}, \tag{32}$$

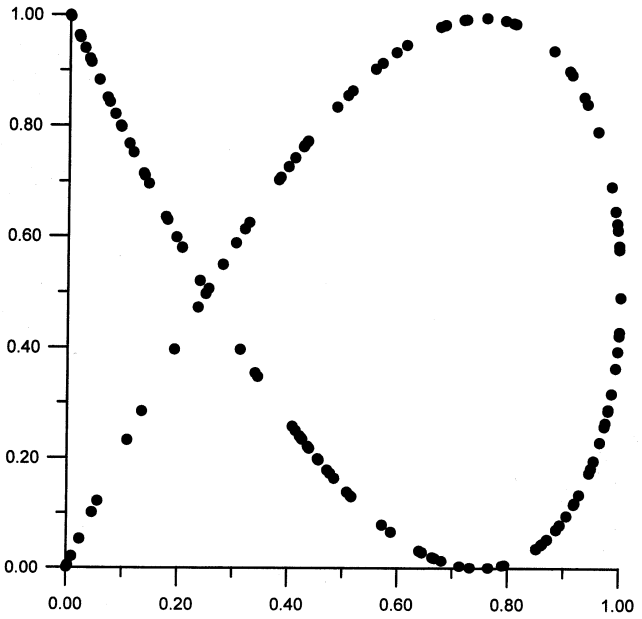

Fig. 8. The return map for the sequence (30) with *z*=3/2.

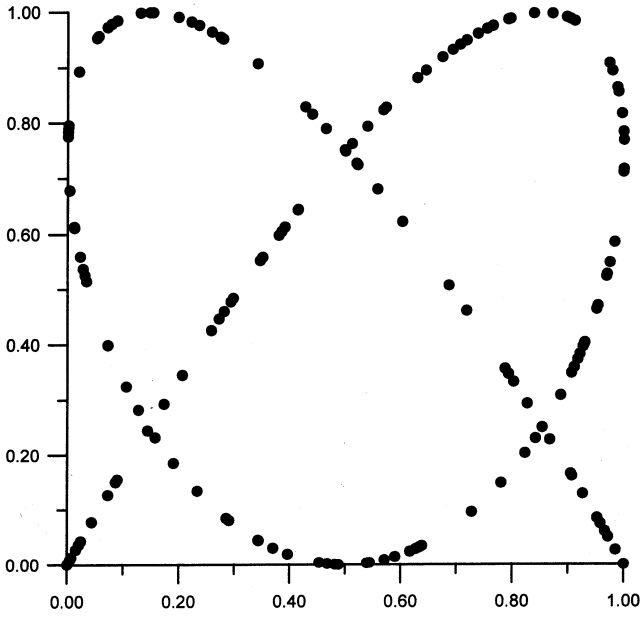

Fig. 9. The return map for the sequence (30) with *z*=4/3.

where *p* and *q* are relative prime numbers, then the first-return map (X_n, X_{n+1}) is the Lissajous curve such that for each value of X_n it has *q* values of X_{n+1} and for each value of X_{n+1} it has *p* values of X_n. Obviously, this relation is not predictable because it is multivalued.

For an irrational parameter *z* in (30), one obtains a set of points of undefined order.

Another possibility of construction of a sequence of non-predictable points is to take in (30) the value *z* of the form

$$z = m^{1/k}, \tag{32}$$

where *m* and *k* are integers, see (González and Pino 2000). Then, the sequence generated,

$$X_n = \sin^2(\pi\theta m^{n/k}), \tag{33}$$

is the solution to the following map equation

$$X_{n+k} = \sin^2(m \arcsin\sqrt{X_n}). \tag{34}$$

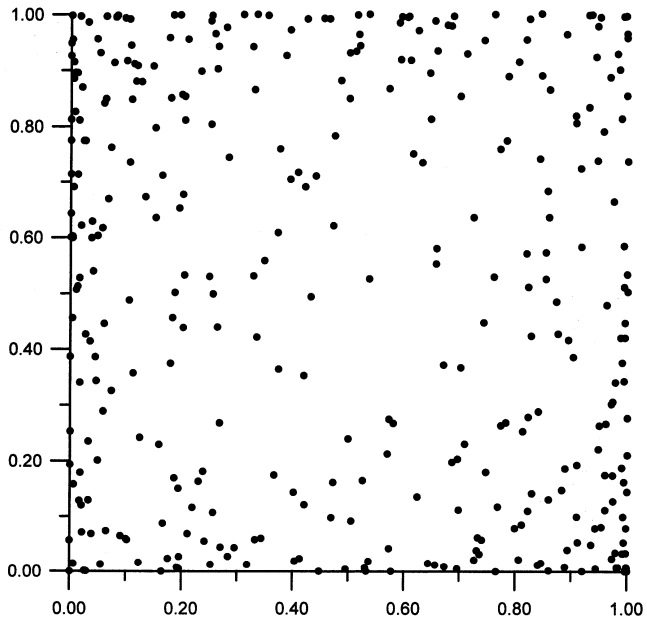

Fig. 10. The return map for the sequence (33) with $m = 2$ and $k = 10$.

Thus, the return map (X_n, X_{n+1}) of this sequence is not predictable while the map (X_n, X_{n+k}) is.

Generation of a realization of the dynamical system (33) needs the assumption of *k* initial values X_0, X_1,..., X_{k-1}. This means that it is the solution of an equation of the form

$$X_{n+k} = f(X_n, X_{n+1}, ..., X_{n+k-1}) \tag{35}$$

The other possibility of ensuring or at least improving practical non-predictability of the constructible (solvable) chaotic dynamical system is increasing the dimension of the state space *S*. For

example, for the construction of the CPRBG we can apply the two-dimensional map, see (Beardon 1991)

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} \sqrt{x_n^2 + y_n^2}\,\cos\left(\sqrt{x_n^2 + y_n^2}\,\arctan\dfrac{y_n}{x_n}\right) \\ \sqrt{x_n^2 + y_n^2}\,\sin\left(\sqrt{x_n^2 + y_n^2}\,\arctan\dfrac{y_n}{x_n}\right) \end{bmatrix}. \tag{36}$$

The recurrence equation (36) has the exact analytic solution

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} \sqrt{x_0^2 + y_0^2}\,\cos\left(\left(\sqrt{x_0^2 + y_0^2}\right)^n\,\arctan\dfrac{y_0}{x_0}\right) \\ \sqrt{x_0^2 + y_0^2}\,\sin\left(\left(\sqrt{x_0^2 + y_0^2}\right)^n\,\arctan\dfrac{y_0}{x_0}\right) \end{bmatrix}, \tag{37}$$

and the two-dimensional dynamical system (37) is chaotic for

$$\sqrt{x_0^2 + y_0^2} \geq 2. \tag{38}$$

The dynamical system map (36) in terms of the complex number radius and the phase angle is

$$F\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} r\cos r\theta \\ r\sin r\theta \end{bmatrix}. \tag{39}$$

To summarize, let us remark that the most poplar congruential random number generator is based on the map

$$X_{n+1} = (mX_n + k) \bmod p, \tag{40}$$

which works in such a way that first expands a natural number (seed) $X_0 \leq p$ to some, possibly greater than p, value and then contracts it again to a value smaller than p. The generators based on exactly solvable or constructible chaotic dynamical systems work in analogous way. The analytical expression for the n-th term of the path first spreads the seed X_0 (belonging to the state space S) over the whole real numbers axis and then contracts the obtained value back to the state space S (since the general expression (27) contains a periodic function). The difference between these generators lies in the fact that the first one is discrete (the arguments and the values of the map are natural numbers) while the second one is continuous (the analogous values are real numbers). The consequence of this fact is that the congruential generators have finite period, usually possible to predict and to make sufficiently large, while the CPRGs have periods theoretically infinite but in fact depending on implementation. Thus, a practical usefulness of a certain constructible dynamical system for construction of the CPRBG should be verified numerically.

NUMERICAL RESULTS AND CONCLUSIONS

For the purpose of this work we have implemented CPRBGs based on the equation (29) with different parameters z and seed values X_0. The dynamical system used in such a generator is quite general and for changing value of the parameter z and, as it was presented in the previous section, it can have quite different properties. The generated bit assumed value zero if $X_{n+1} < 1/2$ and one if $X_{n+1} \geq 1/2$, what seems to be the most natural partition of the state space S. Change of this threshold value could be used to improve the balance between ones and zeros in the generated sequence. In the tested implementation we used the *C++* compiler built-in double precision arithmetic.

Using each generator (constant parameter z, and different seed values) we generated the following sets of bit sequences: 100 files of 10kB, 10 files of 1MB and 1 file of 100MB. In each file we checked the proportion of ones to all generated bits. The results are collected in the Table 1.

The tests of the CPRBGs are still under development, so these results should be treated as early observations. As we can see, when parameter z is close to 1, we get a generator with very poor properties. In the Table 2 we present the results of the tests of the selected CPRBGs.

Analyzing the applied generation procedures and the obtained results of ststistical tests, we see that the algorithms of CPRBGs need additional studies concerning posibilities of hardvare methods of generation (to improve velocity of generators). Moreover, the numerical implementations are very sensitive to the choice of seeds (initial conditions of dynamical systems) and the system parameters; more careful partition of the state space could improve the statistical properties of longer sequences of bits (100 MB). Summarizing, the CPRBGs can be now practically usefull for generation of shorter sequences (e.g., random keys), but still need additional studies for application in stream ciphers.

Table 1.

CPRBG	z	#ones/#bits	remarks[4]
$z > 1$ is an integer parameter (eq. 29)			
1.	2	50% ± 1%	$a = 180$
2.	2	50% ± 1%	$a = 180$, a bit is produced every 10 iterations
3.	2	50% ± 1%	
4.	2	50% ± 1%	a bit is produced every 10 iterations
$z > 1$ is a rational parameter			
5.	$9.24802*10^8$	50% ± 1%	
6.	$5.75582*10^8$	50% ± 1%	
7.	$3.11892*10^9$	50% ± 1%	
8.	$1.47024*10^9$	50% ± 1%	
9.	$2.81175*10^9$	50% ± 1%	
$z > 1$ is a rational parameter, a bit is produced every 10 iterations			
10.	$2.20041*10^9$	50% ± 1%	
11.	$1.41374*10^9$	50% ± 1%	
12.	$1.2353*10^9$	50% ± 1%	
13.	$3.38017*10^9$	50% ± 1%	we observed a few seed value, which lead to sequence of all zeros
14.	$2.86556*10^9$	50% ± 1%	we observed a few seed value, which lead to sequence of all zeros
$z = p / q$ and $z > 1$, where gcd(p, q) = 1 and p, q are integers			
15.	1.35683	only few ones in files	
16.	1.80312	25%	
17.	2.68104	53%	we observed a few seed value, which lead to sequence of all zeros
18.	3.23632	42%	we observed a few seed value, which lead to sequence of all zeros
19.	11.7624	48%	
$z = p / q$ and $z > 1$, where gcd(p, q) = 1 and p, q are integers, a bit is produced every 10 iterations			
20.	3.16946	43%	we observed a few seed value, which lead to sequence of all zeros
21.	1.50937	1%	we observed a few seed value, which lead to sequence of all zeros
22.	1.09814	only few ones in files	almost all seeds lead to sequence of all zeros
23.	4.1407	52%	
24.	1.03221	only few ones in files	almost all seeds lead to sequence of all zeros
$z = m^{1/k}$ and $z > 1$, where m, k are integers (eq.32)			
25.	5.32627	47.5%	we observed a few seed value, which lead to sequence of all zeros
26.	127.543	49%	we observed a few seed value, which lead to sequence of all zeros

[4] Except first two CPRBGs, parameter a is equal to 1

27.	2.50766	57%	
28.	1.81385	30%	we observed a few seed value, which lead to sequence of all zeros
29.	1.0728	only few ones in files	we observed a few seed value, which lead to sequence of all zeros
$z = m^{1/k}$ and $z > 1$, where m, k are integers, a bit is produced every 10 iterations			
30.	1.07303	only few ones in files	almost all seeds lead to sequence of all zeros
31.	4.62611	53%	
32.	16.73	51.5%	
33.	2.92007	55%	
34.	1.49136	only few ones in files	almost all seeds lead to sequence of all zeros

Table 2.

CPRBG	FIPS	Maurer	Chi^2	Linear Complexity	Walsh	Kolmogorov-Smirnov
1	+	-[5]	-[6]	+	+	+
2	+	-[5]	-[6]	+	+	+
3	+	-[5]	-[6]	+	+	+
4	+	-[5]	-[6]	+	+	+
5	+	-[5]	-[6]	+	+	+
6	+	-[5]	-[6]	+	+	+
7	+	-[5]	-[6]			
9	+	-[5]				
10	+	-[5]	-[6]	+	+	+
11	+	-[5]	-[6]	+	+	+
12	+	-[5]	-[6]	+		
25	-	-	-	+		
29	-					
30	-	-	-	-	-	-
31	-	-	-	+	-	+
32	+	-	-[6]	+	+	+
33	-	-	-	+	-	+
34	-	-	-	-	-	

REFERENCES

de Almeida, A. 1988. *Hamiltonian Systems: Chaos and Quantization.* Cambridge University Press, Cambridge.

Beardon, A. 1991. *Iteration of Rational Functions*. Springer-Varlag, New York.

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

Bergé, P., Y.Pomeau, and C.Vidal. 1984. *Order within Chaos.* John Wiley and Sons, New York.

Bollt, E., Y-C.Lai, and C.Grebogi. 1997. "Coding, channel capacity, and noise resistance in

[5] 100MB files did not pass this test
[6] 1MB and 100MB files did not pass this test

communicating with chaos." *Physical Review Letters* 79, no.19: 3787-3790.

Brown, R. and L.O.Chua. 1996. "Clarifying chaos: examples and counterexamples." *International Journal of Bifurcation & Chaos* 6, no.2: 219-249.

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

Devaney, R. 1989. *An Introduction to Chaotic Dynamical Systems.* Addison-Wesley, New York.

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

Ford, J. 1986. "Chaos: solving the unsolvable, predicting the unpredictable." In: *Chaotic Dynamics and Fractals.* M.F. Barnsley and S.G. Demko, eds., Academic Press, New York, 1-52.

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.

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

González, J.A. and R.Pino. 2000. "Chaotic and stochastic functions." *Physica* 276A: 425-440.

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

Gulick, D. 1992. *Encounters with Chaos.* McGraw-Hill, New York.

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

Helleman, R.H.G. 1908. In: *Fundamental Problems of Statistical Mechanics*, vol.5, E.D.G. Cohen, ed., North-Holland, Amsterdam, 165-233.

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

Katok, A. 1980. „Lyapunov exponents, entropy, and periodic points for dipheomorphisms." *Publ. Math. IHES* 51: 137-174.

Katsura, S. and W.Fukuda. 1985. "Exactly solvable models showing chaotic bahavior." *Physica* 130A: 597-605.

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

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

Kohda, T. and A.Tsuneda. 1997. "Statistic of chaotic binary sequences." *IEEE Transactions on Information Theory* 43, no.1: 104-112.

Kotulski, Z. and J. Szczepański. 1997. "Discrete chaotic cryptography." *Annalen der Physik* 6, no.5: 381-394.

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 & Chaos* 9, no.6: 1121-1135.

Li, T.Y. and J.A. Yorke. 1975. "Period three implies chaos." *American Mathematical Monthly* 82: 985-992.

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

Ott, E., C.Grebogi, and J.A. Yorke. 1990. "Controlling chaos.", *Physical Review Letters* 64, no.11: 1196-1199.

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

Pecora, L.M and T.L. Caroll. 1990. "Synchronization in chaotic systems", *Physics Review Letters* 64, no.8: 821-824.

Saber, N.E. 2000. *Discrete Caos.* Chapman & Hall/CRC, Boca Raton.

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

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

Schuster, H. 1988. *Deterministic Chaos.* VCH, Weinheim.

Shilnikov, L. 1984. "Chua's circuit: rigorous results and future problems." *International Journal of Bifurcation & Chaos* 4, no.3: 489-519.

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: 509-528

Szczepański, J., Z.Kotulski, K.Górski, A.Paszkiewicz, and A.Zugaj. 1999a. „On some models of pseudorandom number generators based on chaotic dynamical systems.", *Proceedings RCMCIS'99*, vol.3: 213-220.

Taylor, T.J. 1993. "On stochastic and chaotic motion*.", Stochastics and Stochastics Reports* 43, no.3-4: 179-197.

Taylor, T.J. 1996. "Time series, stochastic and chaotic." In W.A. Barnett (ed.) et al. *Nonlinear dynamics and economisc*. Proceedings of the 10th international symposium in economic theory and econometrics, European University Institute in Florence, Italy, on July 6-17, 1992. Cambridge University Press, Cambridge.

Wieczorkowski, R. and R. Zieliński. 1997. *Computer-aided Random Numbers Generators*, Scientific and Technological Editors, Warsaw. (In Polish.)

Wiggins, S. 1992. *Chaotic Transport in Dynamical Systems*. Springer-Verlag, New York.

Yang, L. Z.Liu, and J.Mao. 2000. "Controlling hyperchaos." *Physical Review Letters* 84, no.1: 67-70.