Arch. Mech., **51**, 3–4, pp. 509–528, Warszawa 1999

Some models of chaotic motion of particles and their application to cryptography*

J. SZCZEPAŃSKI [1], K. GÓRSKI [2], Z. KOTULSKI [1], A. PASZKIEWICZ [2] and A. ZUGAJ [2]

[1] *Institute of Fundamental Technological Research, Polish Academy of Sciences*

[2] *Warsaw University of Technology, Institute of Telecommunication*

IN THE PAPER reflection law models describing the motion of a free particle in a bounded domain are considered. Properties of such dynamical systems are strongly related to the boundary conditions, expressed by a map called a reflection law. We discuss recent results concerning the problem of transferring important properties like chaos, ergodicity and mixing from the reflection law to the motion of the particle. Then we present in a consistent way a method of construction of block cryptosystems, using chaotic reflection law models with appropriate properties. We also propose an application of the mechanical particle model (possessing the transferring property) for constructing pseudo-random numbers generator which can be applied in stream ciphers. The security of the cryptosystem based on particle's motion is due to the property of statistical independence of the actual location of the particle, after a number of reflections, of its initial location.

1. Introduction

DURING THE PROGRESS of civilisation many branches of science of very particular specialisations appeared, so experts in one field do not know what is being done in another. However, it often happens that tools and methods developed in one branch of science can be applied in others, apparently very far away. Let us remember, for example, the use of genetic algorithms in engineering tasks of structural optimisation. In this paper we give another example: the application of non-classical reflection law models, originating from the kinetic theory of dilute gases, for constructing cryptographic algorithms applied in secure communication and information systems.

*The paper has been prepared with the financial support of the Committee of Scientific Research (KBN) under grant no. 8T11D01112

In classical mechanics, the problem of elastic reflection of a moving body from a rigid wall is governed by the fundamental conservation laws, which determine the behaviour of the velocity of the body after the reflection. This gives the following reflection law: the reflection angle is equal to the incidence angle of the body. However, in kinetic theory, where the scale of the reflected bodies (particles) is smaller, the structure of the boundary must be taken into account. Up to now there are only hypotheses as to what happens when the particle reaches the boundary, more or less confirmed by experiment. This results in the necessity of assuming some more complicated boundary conditions for the description of the behaviour of gas particles in a container. The concept of non-classical reflection law models is an attempt at a description of such complicated conditions by some global method.

The theory of non-classical reflection laws found its place in the literature [3, 30, 32, 35, 36, 37]. Reflection law models are an intermediate case between the deterministic systems first considered by SCHNUTE and SHINBROT [32], and the systems with random reflection laws [9]. Namely, we admit a system with strictly deterministic reflection laws that are not one-to-one maps. Thus, in this case it can happen that two different initial configurations in the phase space lead to the same final configuration which is impossible in the Schnute and Shinbrot model. There are a number of maps which can play the role of the reflection law. These and other authors investigated the properties of reflection laws finding that they can lead to non-slip reflection on the boundary, non-increasing entropy, chaos, ergodicity and mixing property of systems describing the behaviour of the particle. These phenomena are examples of a more general effect of transferring chaos (ergodicity, mixing) from some subsystem to an extended system [8, 12, 25, 29, 35, 36, 37].

Non-classical reflection laws found their place in modelling real physical phenomena. A certain interesting physical process governed by a non-classical reflection law was observed and investigated by ANDREYEV [2]. 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 [1], where the theory of the Andreyev reflection law is developed (approaching practical construction of such systems), is the recent paper of NAZAROV [24] devoted to the novel circuit theory of superconductivity.

Problems of transferring some imposed properties from a dynamical system to its extension appear in various situations and seem to be interesting both from the theoretical and practical point of view. They naturally arise from many pro-

blems of engineering dynamics or physics. In general, by an extended dynamical system we understand a system with state space of dimension greater than the original one and functionally dependent on it (e.g. vibrations of a vehicle excited by a working engine). Such a system can be a simple extension of the given dynamical system obtained by adding more co-ordinates without changing the form of the primary ones, or it can be some higher-dimensional dynamical system driven by the lower-dimensional one. Many practical engineering applications dealt with this problem, posed as, for example, the stabilisation of systems by small perturbations (noise or chaos). In this paper we consider the transfer problems in the case of a free particle motion inside a bounded plane domain. We assume the reflection law as a primary dynamical system and the motion of the reflecting particle as an extended system. For our cryptographic applications, the transferring property of "irregularities" in the model used is the basis for constructing a secure algorithm.

Cryptography is a permanent field of interest [31]. At present, the secret communication plays an increasing role in many fields of common life. The basic idea of encryption is to modify the message in such a way that its contents can be reconstructed only by a legal recipient. The message should be represented by a sequence of symbols from a finite alphabet. In practice, the message written e.g. in Latin alphabet, must be transformed, by some known, standard algorithm, to a certain sequence of numbers M (in decimal or binary representation). This procedure is called message encoding. The process of encryption $e(M)$ can be regarded as a function or algorithm producing the ciphertext $C = e(M, k)$. By k we denote a parameter (number), called the secret key chosen at random from a large set. The function inverse to e is the decryption function d, which from the ciphertext C and the secret key k produces the plaintext: $M = d(C, k)$. The security of the algorithm is based on the fact that the decryption is possible only for people who know the secret key k.

One of the fundamental properties of cryptosystems required for their security is statistical independence of plaintexts and the corresponding ciphertexts, strongly connected with the concepts of ergodicity, mixing and chaos [7, 22]. The idea of ergodicity and sensitive dependence on initial conditions (chaos) has its source in the theory of gases (e.g. n-particle models, Lorentz gas, Brownian motion). In the theory, two properties play a fundamental role: ergodicity, that is the convergence of the average value over trajectory to the ensemble mean value, and mixing, which guarantees the convergence from local non-equilibrium to equilibrium state. Analysing the behaviour of individual particles, assuming ergodicity or mixing, we go from any initial conditions of the particles to some macroscopic equilibrium state, where the particles are practically non-discriminable. Therefore, using the reflecting system for encryption, we expect that the position of our particle, describing at its initial state the message being encrypted, after

several reflections will take some non-predictable position and will not be statistically distinguishable from any other possible position, making the algorithm cryptographically secure.

In this paper we present in a consistent way (pointing out the mechanical aspects of the models used) the application of two-dimensional discrete dynamical systems describing the motion of particles, so-called reflection law models, for constructing secure cryptosystems. In the block cryptosystem we take the initial condition of the first coordinate of the system (which describes the position of the particle on the boundary at the moment of reflection) as the plaintext, and the initial condition of the second coordinate (representing the angle of reflection) as the secret key. Both coordinates are iterated; the second, independently of the first, in a chaotic way; the first with some dependence on the second coordinate at each step. For the chaotic dynamical system, taking two initial conditions, we observe an exponential divergence of their trajectories, depending on the distance between the initial conditions of both trajectories. The required statistical properties (ergodicity, mixing) and chaos are obtained in the dynamical system describing the motion of the particle by a transfer from the reflection law.

Except for the results concerning the block ciphers, we suggest an idea of application of the particle motion models for construction of pseudo-random number generators used in the stream cipher. In the models, the required property of the system could be obtained by the transferring process. The basic idea of bit generation is that the actual location of the particle (in a phase space) indicates which bit we choose: "0" or "1". We hope that such a theoretical construction (usually simulated in the computers) can be further developed to some physical realisation, slightly increasing the speed of generation of bits and avoiding the computer calculations errors.

2. Reflection law models

To establish a reflection law model, one must select a domain with a certain shape of the boundary and define the reflection law. 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. From this point of view, non-classical reflection laws need not satisfy such a fundamental physical law as the conservation of linear momentum. However, one can find some situations where such laws can describe realistic physical phenomena. Consider for example a container, the wall of which has some microstructure (Fig. 1). We assume that the mass of the reflected particle is negligible in comparison to the mass of the container. Then the reflection process, observed as non-classical, can in fact be the effect of several classical elastic reflections where, for every micro-

reflection, the conservation of linear momentum is satisfied. In this model, due to the small scale of the microreflection, we identify the outgoing position with the incoming position. The reflection law is usually quite general and it can be written symbolically as:

$$\nu_{\text{ref}} := T_x(\nu_{\text{inc}}), \tag{2.1}$$

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

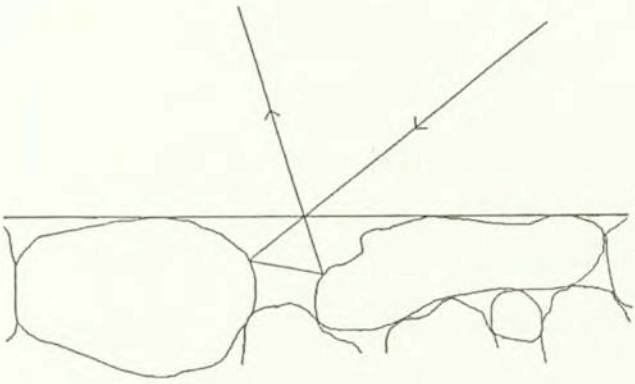

FIG. 1. Effect of the boundary microstructure on the reflection law.

In our considerations we assume that the particle moves with a constant velocity, changing only the direction at the moment of reflection. In the particular case of the reflection law conserving the angle of incidence (the angle of incidence is equal to the angle of reflection), one obtains the class of dynamical systems called billiards. This conservative reflection law (as a map) is neither ergodic nor chaotic [35]. (However, it is well known that in appropriate domains it can lead to ergodic or chaotic motion of a particle.) Thus, to obtain ergodic [7] and chaotic properties [29] of a reflection law, one must assume another map relating the incident and outgoing angles. In this paper we consider the reflection law models in two dimensions, where we can observe the qualitative results we are interested in, especially the transferring property. We approximate the boundary of the plane domain of particle's motion by some closed, sufficiently smooth curve. Extensions of the results in two dimensions to more-dimensional spaces lead to some technical problems, which can be also observed in the case of the widely studied classical billiards theory. However, the results in $\mathbb{R}^2$ can give some suggestions concerning the behaviour of more-dimensional systems.

In order to get the simplest form of equations of particle motion, we use the following co-ordinate system introduced by BIRKHOFF [5]: (x_n, ν_n), where x_n denotes the position of the particle on the boundary at the moment of the n-th reflection, and ν_n is the angle between the velocity of the particle after the

reflection and the tangent to the boundary at x_n (see Fig. 2) [7, 36, 37]. 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 $T_x(.)$ (under some assumptions, a dynamical system itself). Thus, $F_T(.,.)$ acts from the product of two intervals onto the same product:

$$F_T : [0, L) \times (0, \pi) \to [0, L) \times (0, \pi) \tag{2.2}$$

and can be written in the following form:

$$(x_{n+1}, \nu_{n+1}) = F_T(x_n, \nu_n). \tag{2.3}$$

The symbol L in Eq. (2.2) denotes the length of the boundary of the domain.

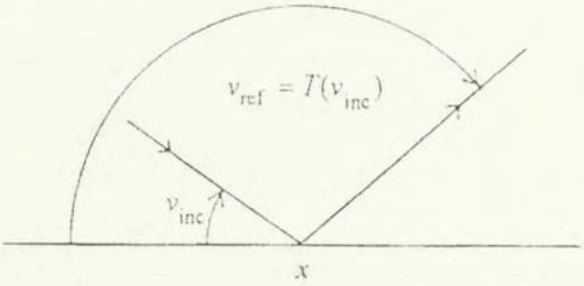

FIG. 2. The reflection law in local coordinates.

In our further considerations the reflection law $T_x(.)$ is assumed to be independent of x (which means that the properties of the walls of the container are identical at every point x),

$$T_x(.) \equiv T(.). \tag{2.4}$$

Then the reflection law $T(.)$ is a one-dimensional dynamical system itself and it is used for construction of the two-dimensional dynamical system $F_T(.,.)$. It is interesting to know, how properties of the smaller system $T(.)$ affect the larger one – $F_T(.,.)$, which describes the motion of a particle in the container.

3. Transferring problems

In the previous section we considered reflection laws as dynamical systems with certain properties. If the reflection law extracted from the extended dynamical system describing the motion of a freely moving particle is independently considered, one can ask the following questions: what are the properties of the extended system if we use a non-classical reflection law? What is the effect of the specific properties of the reflection law (like chaos or ergodicity) on the behaviour of the particle? Is the particle motion chaotic or ergodic? In our model

the shape of the boundary also affects the properties of motion and it leads to a new question: what is the influence of the shape of the container on the motion of the particle? In this section we present some interesting results concerning the above problems.

To give some insight into transferring properties we study this phenomenon in two typically used containers: a circle and a square. In the case of a circle, after simple geometrical considerations, making use of the rotational symmetry, we obtain the following system of evolution equations:

$$\begin{aligned} \nu_{n+1} &= T(\nu_n), \\ x_{n+1} &= x_n - 2\nu_{n+1} (\mathrm{mod}\ 2\pi), \end{aligned} \tag{3.1}$$

where $x_n \in [0, 2\pi)$, $\nu_n \in (0, \pi)$. The first equation constitutes a reflection law and the second one is inherently connected with systems of such type. It turned out [36] that in this model, ergodicity (and also chaotic behaviour) of a reflection law implies ergodicity (chaos) of the trajectories of a particle. Moreover, if the reflection law has an attracting periodic orbit then the trajectories of moving particles are asymptotically periodic.

Related questions were studied in the context of Brownian motions and also as a purely mathematical problem. In [4] a class of non-linear dynamical systems describing the motion of a particle in a viscous liquid under the influence of a kick force was investigated. In this case the time evolution of velocity of the particle is governed by the system of equations:

$$\begin{aligned} x_{n+1} &= T(x_n), \\ y_{n+1} &= \lambda y_n + f(x_n). \end{aligned} \tag{3.2}$$

It was proven [4] that under appropriate conditions on the map $T(.)$, the force $f(.)$ and the constant λ ($|\lambda| < 1$ depends on the viscosity of the liquid) periodicity, ergodicity and the mixing property (see Sec. 5 for definitions) of $T(.)$ imply the same properties of the extended dynamical system (3.2). The variable y_n in Eq. (3.2) corresponds to the velocity of the kicked particle and the ergodic (periodic, mixing) property is supported by the vicinity consisting of other particles (whose evolution is governed by $T(.)$ through the force $f(.)$). In our model (3.1), ergodicity (periodicity, chaos) is transmitted to the velocity of the particle from the boundary of the container by means of the reflection law.

The equation (3.1) has another interesting physical interpretation. It turned out that this evolution equation is topologically conjugated [37] to the well-known "standard maps" (see [23, 34] and the literature therein), for the first time introduced by the physicists B.V. Chirikov and J.B. Taylor. The standard maps appear

in many situations; they are obtained as a Poincaré map describing the motion of an electron rotating in the plane perpendicular to a uniform magnetic field in circular accelerators [13, 14].

Considering our second model of the container, that is the square, we come to quite different results concerning the transferring property. We show that if we assume $T(.)$ to be a unimodal map, for example:

$$\nu_{n+1} = T(\nu_n) = \frac{4}{\pi}\nu_n(\pi - \nu_n), \tag{3.3}$$

then in the square the transferring problem reduces to the study of dynamical systems given by the following one-dimensional map:

$$G = T \circ h : [0, \pi] \to [0, \pi], \tag{3.4}$$

where h is some involution, i.e.

$$h^2(\nu) = \nu \quad \text{for every} \quad \nu \in [0, \pi]. \tag{3.5}$$

We proved that in the square containers, ergodic and chaotic reflection laws $T(.)$ can even lead to some periodic motion of the particle [37]. This result can be generalised to containers with convex polygon boundaries.

The interesting question is if for a given container, equivalent reflection laws (topologically conjugated) lead to the same qualitative properties of the motion of the particle. We found [35] two topologically equivalent reflection laws, both ergodic and chaotic which in the square domain transfer to the extended system in completely different ways. For the first law, the motion of the particle is asymptotically periodic, that is the particle tends to some fixed periodic orbit. In contrast, for the second reflection law and almost all initial points (x_0, ν_0), the set of velocities $\{\nu_n, n = 1, 2, ...\}$ corresponding to each initial point is dense in a set of Lebesgue measure of at least $\pi/2$.

In Sec. 5 we give an example of a reflection law satisfying the transferring property in the square, which is useful for our cryptographic purposes. It is interesting to find some general assumptions on the reflection law that assure the transferring property for a large class of containers. It seems that these types of reflection laws could be interesting from a physical point of view.

4. Elements of cryptology

Before we start the presentation of a cryptographic algorithm taking its source from some mechanical phenomena or, more precisely, from the theory of rarefied gases, we introduce the definitions of fundamental terms needed for understanding the procedures. The first procedure, preceding the encryption, is a coding algorithm. It is the method of translation of the natural message (spoken

or written) into a sequence of numbers. This can be for example the representation of letters and numbers by the ASCII code in digital computers, or transfer of human voice to a sequence of binary pulses in telephone communication. When the message is coded, i.e. represented in the form of a sequence of numbers (decimal or binary), it can undergo some additional transformation, which makes it non-understandable for everyone except the intended recipient. This is the field of interest of cryptology.

Cryptology is the branch of science [31] dealing with the design of encryption algorithms and the investigation of their strength (by studying methods of breaking them). Cryptology has been of some interest at all times. Mostly it has been used in connection with military or diplomatic affairs and for instance, in its early stages it was almost exclusively concerned with secretly written information. With the development of an ever refined communication technology, nowadays secret communication plays also an increasing role in commercial, industrial and banking sectors. It is due to the actually increasing importance of cryptology in economics that the research activities in the field and the search for new cryptographic methods still continues.

Cryptography is the process of transforming information (plaintext) into unintelligible form (ciphertext) so that it may be sent over insecure channels or it may be stored in insecure files. Cryptographic procedures can also be used for personal identification, digital signatures, access control etc.

A cryptosystem is a cryptographic algorithm, which is usually known, and which depends on some parameter called the key. With encryption we can transform the plaintext to a form which an outsider cannot interpret unless he knows the method and the key used in the process. Decryption is the inverse process in which encrypted data are translated to clear data. Thus, a cryptosystem is a two-way procedure: encryption – decryption. Let us also remark, that the coding procedure must be also two-way. If we precede the encryption algorithm with some encoding procedure, then we must follow the decryption with some decoding, inverse to the encoding process.

There are two types of encryption algorithms: stream ciphers and block ciphers [31]. A stream cipher is a method in which we have some secret key generator which produces a bit stream (the key stream) which enciphers the plaintext bit stream by simple modulo 2 addition. The stream cipher system thus hides the plaintext by changing the bits of it in a random-like way. An interceptor, who does not know the key, will not know which bits have been changed (corresponding to the occurrence of "1" in the key stream), and which ones remain unchanged ("0" in the key stream). Unlike stream ciphers, where only one bit at a time is encrypted, in block ciphers whole blocks of bits are treated simultaneously. In this case the plaintext information is hidden by the fact that, depending on the key, a ciphertext block can be deciphered to any combination of plaintext bits

or to as many combinations as there are keys. If the keys are chosen with equal probability, then to the interceptor observing a ciphertext block, all the possible plaintext blocks are equally likely to have occurred.

5. Chaotic dynamical systems - new tool for cryptology

In recent years a new approach to constructing cryptosystems based on application of the theory of both continuous and discrete chaotic dynamical systems has been developed. Within the continuous theory, methods of synchronisation of chaotic systems [15, 16, 27, 28] and the idea of controlling chaos [11, 15, 26] are applied. In the discrete systems approach, the constructions of cryptosystems based on iterations and inverse iterations of chaotic maps (with possible methods for introducing keys) are developed.

The earliest applications of chaotic systems in cryptography were proposed by PECORA and CAROLL in 1990 [28] as a possible application of the synchronisation of chaotic dynamical systems. This idea has been developed by KOCAREV *et al.* [16] and PARLITZ *et al.* [27], where an experimental test system based on chaotic electronic circuits was presented. The first paper employed analogue signals while the second one used binary signals. An overview of the methods connected with encrypting messages with the modulation of trajectories of continuous dynamical systems can be found in [15].

Application of discrete chaotic dynamical systems to cryptography was first analysed by HABUTSU *et al.* [10] and then developed by KOTULSKI and SZCZEPAŃSKI [19, 20]. Before we present the algorithm of encryption and decryption, we introduce all the required properties and definitions.

Chaos is the property of sensitive dependence of trajectories of the dynamical system on the initial conditions [22, 34]. More precisely, a non-linear system is chaotic if it has positive Lyapunov exponents in a certain domain. Consider for example a one-dimensional dynamical system (I, φ), where φ is a C^1 -class map transforming the interval I into itself. If at some point $x \in I$, the Lyapunov exponent $\lambda_x > 0$, then

$$(5.1) \qquad \forall \varepsilon > 0 \exists n_1, n_2 \exists U_{n_1,n_2} \ni x, \forall n_1 \leqslant n \leqslant n_2, \forall z_1, z_2 \in U_{n_1,n_2}$$

$$\exp\{(\lambda_x - \varepsilon)\, n\}\, |z_1 - z_2| < |\varphi^n(z_1) - \varphi^n(z_2)| < \exp\{(\lambda_x + \varepsilon)\, n\}\, |z_1 - z_2|,$$

where U_{n_1,n_2} is some neighbourhood of $x \in I$. The above expression 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 $\exp\{(\lambda_x - \varepsilon)\, n\}$ times.

Let us illustrate the idea of including the secret key into the initial condition by some elementary one-dimensional example [19]. Let γ be a one-dimensional

chaotic map with positive Lyapunov exponent λ:

$$\gamma : [0,1] \to [0,1], \tag{5.2}$$

and $P \in (0,1)$ be the message to encrypt. Fix a natural number n (number of iterations) and choose the secret key $k \in (0,1)$. Let $\overline{C}$ be some selected pre-image of P under the map γ^n:

$$\overline{C} = \gamma^{-n}(P); \tag{5.3}$$

$$\gamma^n(\overline{C}) = \gamma^n\left(\gamma^{-n}(P)\right) = P. \tag{5.4}$$

Then, we calculate C, the ciphertext of P as

$$C = \overline{C} + k (\mathrm{mod}\, 1). \tag{5.5}$$

Decryption is the inverse operation, that is

$$P = \gamma^n(C - k). \tag{5.6}$$

An outsider tries to approximate the key k assuming some value of the secret key, say k_1 such that $|k - k_1| < 10^{-20}$. Then he calculates the value of plaintext $P_1 = \gamma^n(C - k_1)$. For $n = 30$, $\lambda - \varepsilon \approx 1.558$ (which is a reasonable value for many dynamical systems), due to chaos we have:

$$|P - P_1| = |\gamma^n(C - k) - \gamma^n(C - k_1)| \geqslant e^{n(\lambda - \varepsilon)}\, |k - k_1| \approx 0.5. \tag{5.7}$$

Formula (5.1) and the above example suggest how to choose a chaotic map with suitable Lyapunov exponent to construct DDC cryptosystem. First we select an admissible class of maps (with respect to possibility of practical implementations), e.g. of parabolic type, and establish the number of iterations n to guarantee the required speed and accuracy of calculations. Then we fix the map with the Lyapunov exponent such that the obtained speed of divergence (governed by formula (5.1)) makes ciphertexts corresponding to close plaintexts completely different. For example, for $n = 30$, the accuracy equal to 10^{-20}, the estimation (5.7) shows that the map with the Lyapunov exponent $\lambda \approx 1.6$ could be used.

The formula (5.7) demonstrates how the chaos property protects the system against a brute force attack (where the algorithm is tested with all possible secret keys). However, cryptoanalysts use some more sophisticated attacks to break cryptosystems. To make the cryptosystem based on the chaos property more robust against statistical cryptoanalytical attacks, we postulate some other important properties of the applied dynamical system, like ergodicity and mixing property. For cryptographic purposes we shall use dynamical systems with invariant measure equivalent to the Lebesgue measure.

We say that the measure μ is invariant, if and only if it satisfies

$$\forall A \in \sigma(X), \qquad \mu(A) = \mu(\varphi^{-1}(A)). \tag{5.8}$$

We postulate that μ is equivalent to the Lebesgue measure, i.e.:

$$\forall A \in \sigma(X), \qquad \mu(A) = \int_A g(x)dx, \tag{5.9}$$

with its density function $g(.)$ satisfying for all x the following condition:

$$0 < g_1 \leqslant g(x) \leqslant g_2, \tag{5.10}$$

where g_1 is close to g_2.

We say that (X, φ) is ergodic if and only if it has only trivial invariant sets, i.e., if $\varphi(B) \subset B$ then $\mu(B) = 0$ or $\mu(B) = \mu(X)$. The ergodicity implies that the state space cannot be nontrivially divided into several parts. Therefore if some trajectory starts from any point x, it never localises in a small region. It means that the plaintext space which can correspond to a given ciphertext cannot be restricted to a "smaller" subspace (smaller than X). Thus, for the ciphertext C the corresponding plaintext P (during brute attack) must be searched for over all the state space X. We can also postulate a stronger condition, assuring better probabilistic properties of the set of possible ciphertexts. The system is mixing if the following condition is satisfied (we assume that $\mu(X) = 1$) for any sets A and B:

$$\lim_{n\to\infty} \frac{\mu(\varphi^{-n}(A) \cap B)}{\mu(B)} = \frac{\mu(A)}{\mu(X)}. \tag{5.11}$$

This property means that the part of B which after n iterations of φ will be contained in A, is asymptotically proportional to the ratio of A in X with respect to the measure μ. Thus for any ciphertext C, all the possible plaintexts P (during brute attack) are μ-equiprobable.

6. A new type of block ciphers – the DCC algorithm

In this section we outline the application of our encryption algorithm using the reflection law model. The first step is the coding procedure, where the message expressed in natural language (a sequence of symbols from a finite alphabet) is transformed to a binary sequence by some public method. Then the sequence is divided into finite blocks of bits of the same length. Now we can identify the usual elements of a block cryptosystem. We assume, that every plaintext is some number $P \in (0, 1)$, the secret key is the parameter k – a number from some interval (usually also a representation of some finite binary sequence). The ciphertext is also a number, $C \in (0, 1)$.

In the general formulation of the DCC cryptosystem we use some chaotic map $\varphi_k(.)$, depending on the parameter k,

$$\varphi_k : (0,1) \to (0,1). \tag{6.1}$$

The encryption is the n-fold iteration of the inverse map φ_k^{-1} with the initial value P according to some (secret, determined by k) rule of choices of the successive pre-images of φ_k^{-1}. The ciphertext C is obtained as:

$$C = \varphi_k^{-n}(P) = \varphi_k^{-1}(\varphi_k^{-1}(...\varphi_k^{-1}(P))). \tag{6.2}$$

The sender encrypts all the blocks of the coded message, say P_i, $i = 1, 2, ..., m$, using the secret key k and obtains the sequence of ciphertexts C_i, $i = 1, 2, ..., m$. The ciphertexts are sent by an open channel to the recipient. The legal recipient (person, who knows the secret key k), to obtain the plaintext performs the following decryption algorithm using the n-th iteration of the map φ_k:

$$P = \varphi_k^n(C) = \varphi_k(\varphi_k(...\varphi_k(C))) \tag{6.3}$$

He does this for all C_i, $i = 1, 2, ..., m$ and obtains the plaintext which is the coded message. The final step is the application of the decoding procedure, inverse to the initial coding step. It is obvious that the above construction of DCC block cryptosystems can be generalised to more dimensions (more dimensional spaces of plaintexts and ciphertexts).

There are two possibilities of introducing the secret key k into the algorithm. First, k can be an internal parameter of the map φ [10], second, k can be included into the initial condition [19, 20].

The map $\varphi(.)$ applied in (6.2) – (6.3) is quite general. However, to assure sufficient security of the cryptosystem we should apply maps that are chaotic, ergodic and even mixing. Maps describing particle's motion governed by appropriate reflection laws have the required properties and after some adaptation they can be applied for constructing secure cryptosystems.

To construct a concrete reflection law model useful for cryptographic purposes, we must take into account not only security but also the computational aspects – in this case the accuracy of numerical calculations and computational complexity. Therefore we propose the square as a domain and a piece-wise parabolic reflection law to construct the reflection law model. In the system the state variable is the pair (x, ν), where $x \in [0, L)$ represents the message evolving (during encryption) iterations from the plaintext P to the ciphertext C (we identify x with the distance of the particle's reflection point from some fixed point of the square measured along the sides of the square), and $\nu \in (0, \pi)$ is the reflection

angle. We take the reflection law T_D of the following form:

$$T_D(\nu) = \begin{cases} \dfrac{\nu^2}{\pi} + \dfrac{3\nu}{2} & \text{for } \nu \in \left(0, \dfrac{\pi}{2}\right), \\ \dfrac{\left(\nu - \dfrac{\pi}{2}\right)^2}{\pi} + \dfrac{3\left(\nu - \dfrac{\pi}{2}\right)}{2} & \text{for } \nu \in \left[\dfrac{\pi}{2}, \pi\right). \end{cases} \tag{6.4}$$

This map is chaotic, ergodic and even mixing [18]. For $T_D(.)$ these properties transfer to the larger system describing the motion of a particle as required.

Thus, a general form of the two-dimensional dynamical systems, describing the motion of a particle that we use for construction of the cryptosystems, is $F_{T_D}(x, \nu) = (S(x, \nu), T_D(\nu))$. The inverse iterations of this system are the steps of encryption. During encryption, the first co-ordinate describes the evolution of the message and the second one – the evolution of the secret key. Decryption involves forward iterations transforming the position representing the ciphertext to the one corresponding to the plaintext. As before, the second co-ordinate describes the evolution of the secret key. The details of the algorithm together with the results of numerical experiments can be found in [21].

7. DCC as a pseudo-random number generator

The chaotic dynamical systems with good properties can be used for constructing pseudo-random sequences of bits [17], being, among other applications, the foundation for construction of stream cryptosystems. As we mentioned, such sequences (called the secret key streams) hide the content of the original binary message by changing the value of a bit to the opposite, if the corresponding bit of the key stream is 1 and leaves it unchanged if the corresponding bit of the key stream is 0. An ideal stream cipher would use some physical system (true random number generator) as a key stream generator. However, since its output cannot be reproduced, decryption (the operation which in the case of a stream cipher is the repetition of the same algorithm as in encryption with the same key stream) would be impossible unless the whole key stream would be transported to the legitimate recipient via a secure channel. This procedure is often impractical, therefore mostly so-called pseudo-random number generators with special properties, controlled by a relatively short key (called the seed), have to be used as key stream generators (instead of physical generators commonly used).

The most important property of the binary sequences used as the key streams, guaranteeing the security of the cryptosystems, is impossibility of reconstruction or prediction of unknown bits on the basis of a known sequence of bits. In other words, the key stream must have properties analogous to a white noise process, that is independence of its states for different instants of time. As is known,

the concept of white noise is strongly connected with a description of a particle's motion called the Brownian motion. This fact indicates a possibility of application of the reflection law models. To assure good statistical properties of the generated sequences we propose to make use of the physical systems with transferring phenomena, where the required properties (e.g. mixing, chaotic behaviour) of a smaller system affects the extended one, describing globally the physical process.

Consider the motion of a particle in the square with the reflection law given by (6.4). In this case the state space is the Cartesian product of two intervals:

$$S = [0, L) \times (0, \pi). \tag{7.1}$$

The basic idea of the method is the following. We divide (in some appropriate way) the state space S of the reflection law model into two parts S_0, S_1 ($S_0 \cup S_1 = S$). We start observation of the evolution of the particle starting from an initial state (x_0, ν_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 iteration in the set S_0, that is $(x_n, \nu_n) \in S_0$, and "1" otherwise.

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

$$\mu(S_0) = \mu(S_1) = \frac{1}{2}. \tag{7.2}$$

(In our investigations we assumed $S_0 = \left\{(x, \nu) \in S, |x| < \frac{L}{2}\right\}$). Then, by condition (7.2) 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 [7], which for our reflection law model can be written as:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} p\left(F_{T_D}^i(x_0, \nu_0)\right) = \int_S p d\mu, \tag{7.3}$$

(for almost all $(x_0, \nu_0) \in S$ with respect to μ), where p is an arbitrary μ – integrable function. Taking as the function p the indicator function of the set S_1, that is

$$p(.) = \chi_{S_1}(.), \tag{7.4}$$

we obtain that in the pseudo-random sequence determined by the seed

$(x_0, \nu_0) \in S$, the average number of "1" is:

$$\frac{1}{n}\sum_{i=0}^{n-1} \chi_{S_1}\left(F^i_{T_D}(x_0,\nu_0)\right) \underset{n\to\infty}{\longrightarrow} \int_S \chi_{S_1} d\mu = \mu(S_1) = \frac{1}{2}, \tag{7.5}$$

due to (7.2). This condition guarantees that both values in the sequence of bits, that is "1" and "0" are equiprobable and any illegal recipient has no *a priori* indication concerning the sequence. Now we should show that bits of the generated sequence are statistically independent, which practically assures the impossibility of determining some bit on the basis of some others. To show this we use the mixing property.

Define the random variable B_n, responsible for the generation of the n-th bit, in the following way:

$$B_n(x_0,\nu_0) = \chi_{S_1}(F^n_{T_D}(x_0,\nu_0)), \tag{7.6}$$

where the set S is the space of elementary events and the normalised invariant measure μ is the probability distribution describing our binary random variable B_n:

$$B_n : S \to \{0,1\}. \tag{7.7}$$

For every n, the probabilities that the random variables B_n are equal to "1" and "0" are:

$$P(B_n = 1) = \mu\left(F^{-n}_{T_D}(S_1)\right), \qquad P(B_n = 0) = \mu\left(F^{-n}_{T_D}(S_0)\right) \tag{7.8}$$

respectively. Applying the mixing property (5.11) we can show asymptotic independence of random variables B_n and B_{n+m} for m sufficiently large. Then, taking the modified dynamical system $G_{T_D}(.,.)$:

$$G_{T_D}(x_0,\nu_0) := F^m_{T_D}(x_0,\nu_0) \tag{7.9}$$

in definition (7.6) instead of F_{T_D}, we obtain the sequence of statistically independent random bits.

Generating bits according to the proposed algorithm we require the complete repeatability of the obtained sequences (what is the necessary condition of correct decryption in the stream cipher methods). In practical implementations the numbers used in calculations are expressed with some accuracy. Therefore, if our moving particle is close to the boundary of separation of the sets S_0 and S_1, then the numerical error can make that "0" generated in one computer becomes "1" in another (or *vice versa*). The idea of how to prevent this inconvenience was presented in [6]. The authors suggest to introduce a forbidden gap of small size at the partition $S_0 - S_1$ boundary an then to neglect all the trajectories which

go through this gap. For some chaotic maps describing the dynamical systems it is possible to characterize the forbidden trajectories imposed by the dynamics itself. 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.

We presented the construction of a single pseudo-random sequence described by the seed $(x_0, \nu_0) \in S$ (which is the elementary event in our model). We showed that statistical properties of such a sequence are sufficiently good for cryptographic purposes. In practice users of a stream cryptosystem need a large number of sequences. We can generate them by changing the initial conditions (seeds). Using the mixing property (provided by transferring phenomenon) of the reflection law models we can show that two sequences (corresponding to two different seeds) are different; moreover, by the chaos we obtain, that they cannot overlap over long sub-sequences of bits. Thus we have presented a method of generating bits which can be quite useful in practical applications.

8. Conclusions

Reflection law models arise in a natural way in the theory of rarefied gases (Knudsen gases) [3, 36], in description of particle's motion in accelerators [13, 14, 23] and in mesoscopic models of superconductive media [2, 24]. In the first case the model takes into account the behaviour of the gas particles at the boundary and the shape of the container (which is important, because we neglect the mutual interactions of the particles). Investigating the accelerators one finds that the corresponding Poincaré maps (being the standard maps) are topologically conjugated to some reflection law models. The theory of standard maps [23, 34] is extensively investigated in the literature. Authors studied the coexistence problem [34], that is the possibility of simultaneous existence of chaotic and regular trajectories in the same system. Another important problem is the transferring of certain properties of a smaller system to the larger one. In our paper this phenomenon was studied in the context of the effect of boundary conditions (represented by the reflection law) on the motion of the particle described by the reflection law model. We studied the possibility of transfer of chaotic, ergodic and mixing behaviour of the dynamical system modelling the reflection law to the dynamical system describing particle's motion (the reflection law model). We found that, under some additional assumptions concerning the reflection law and the shape of the container, the reflection law model governed by some chaotic, ergodic and mixing reflection law can have the same properties. However, we also observed an unexpected effect where the chaotic reflection law leads to regular

(even periodic) motion of the particle [37]. It is the interesting problem to construct chaotic and mixing reflection laws which guarantee the transfer of these properties to dynamical systems describing the motion of a particle in a large class of containers.

In the second part of our paper we gave a practical application of the observed effects. Among recent uses of chaos one can find also secure communicatons [15]. In [19, 20] we proposed a method of extending discrete dynamical sysems for constructing secure cryptosystems. The algorithms presented in this paper are examples of a realisation of the general scheme with application of the reflection law model [21]. The applied unified approach using the theory of abstract dynamical systems made it possible to prove the security of the proposed cryptosystems. Mathematical tools used for this purpose are quite general and hey are extensively studied in the literature. This new approach allowed us to obtain rigorous mathematical results concerning the cryptosystems (especially theirstatistical properties) but on the other hand, it opens a new area of investigaions in the theory of dynamical systems in the context of secure communications.

The presented DCC algorithm is an idealised model. In practice, developing software implementations, one should take into account the usual computational restrictions [31, 33]. Since numbers in digital computations have a finite representation, one must assume the lengths of computed values (key, plainext, ciphertext) such that both the forward iterations and inverse iterations can be performed uniquely and in such a manner that one can obtain the required number of significant bits of plaintext in the decryption process. In other words one must fix the information rate R

$$R = \frac{\text{plaintext size}}{\text{ciphertext size}}$$

specific for the algorithm applied and the computer accuracy. Therefore, devlopment of programs implementing our algorithms and useful in advanced pracical applications need some additional investigations taking into account this aspect of the problem. From the other side, it could be promising to consider a posibility of construction of physical systems realising our cryptographical algoritms. In spite of the fact that, in this case, we avoid the problem of computation erors, we face another one – the accuracy of measurements.

References

1. B.L. ALTSHULER, P.A. LEE and R.A. WEBB, *Mesoscopic Phenomena in Solids, series Modern Problems in Condensed Matter Sciences*, vol. **30**, North-Holland, Amsterdam 191.

2. A.F. ANDREYEV, *Thermal conductivity of the intermediate state of superconductors*, Zh.Exp.Theor.Fis., **46**, 1823–1828, 1964.

3. H. BABOVSKY, *Initial and boundary value problems in kinetic theory. I. The Knudsen gas, II. The Boltzmann equation*, Transp.Theor.Stat.Phys., **13**, Part I-455–474, Part II-475–498, 1984.

4. C. BECK, *Ergodic properties of a kicked damped particle*, Comm.Math.Phys., **130**, 51–60, 1990.

5. G.D. BIRKHOFF, *Dynamical Systems*, New York 1927.

6. E. BOLLT, Y-CH. LAI and C. GREBOGI, *Coding, channel capacity and noise resistance in communicating with chaos*, Phys. Rev. Lett., **79**, 19, 3787–3790, 1997.

7. I.P. CORNFELD, S.V. FOMIN and YA.G. SINAI, *Ergodic theory*, Springer-Verlag, Berlin 1982.

8. M.S. EL NASCHIE, *Complex dynamic in a 4D Peano-Hilbert space*, Il Nuovo Cimento, **107B**, 5, 583–594, 1992.

9. S. GOLDSTEIN and C. KIPNIS, N. IANIRO, *Stationary states for a mechanical systems with stochastic boundary conditions*, J. Stat. Phys. **41**, 915, 1985.

10. T. HABUTSU, Y. NISHIO, I. SASASE and S. MORI, *A secret key cryptosystem by iterating a chaotic map*, EUROCRYPT'91, 127–140.

11. S. HAYES, C. GREBOGI and E. OTT, *Communicating with chaos*, Physical Review Letters, **70**, 20, 3031–3034, 1993.

12. K. HIKAMI, P.P. KULISH and M. WADATI, *Integrable spin systems with long range interactions*, Chaos, Solitons & Fractals, **2**, 5, 543–550, 1992.

13. J.M. HOWETT, M. MONTH and S. TURNER, *Nonlinear dynamics, aspects of particle accelerators*, Proceedings, Sardinia, Lecture Notes in Physics, Springer, Berlin 1985.

14. Y.H. ICHIKAVA, T. KAMIMURA, T. HATORI and S.Y. KIM, *Stochasticity and symmetry of the standard map*, Prog.Theor.Phys., Supplement, **98**, 1–18, 1989.

15. T. KAPITANIAK, *Controlling chaos, Theoretical and practical methods in non-linear dynamics.*, Academic Press, London 1996.

16. LJ. KOCAREV, K.S. HALLE, K. ECKERT, L.O. CHUA and U. PARLITZ, *Experimental demonstration of secure communications via chaotic synchronisation*, Int.J.Bifurc. & Chaos, **2**, 709–713, 1992.

17. T. KOHDA and A. TSUNEDA, *Statistics of chaotic binary sequences*, IEEE Transactions on Information Theory, **43**, 1, 104, 1997.

18. A.A. KOSJAKIN, E.A. SANDLER, *Ergodic properties of some class of piecewise smooth maps on the interval*, Matiematika, **3**, 32–40, 1972.

19. Z. KOTULSKI and J. SZCZEPAŃSKI, *Discrete chaotic cryptography*, Annalen der Physik, **6**, 5, 381-394, 1997.

20. Z. KOTULSKI and J. SZCZEPAŃSKI, *Discrete chaotic cryptography (DCC). New method for secure communication*, Proc.Non-linear Evolution Eequations and Dynamical Systems '97, Crete, Grece, http://www.roma1.infn.it/ ragnisco/proc97.htm, 1997.

21. Z. KOTULSKI, J. SZCZEPAŃSKI, K. GÓRSKI, A. PASZKIEWICZ and A. ZUGAJ, *Application of discrete chaotic dynamical systems in cryptography – DCC method*, International Journal of Bifurcation and Chaos, **9**, 6, 1121–1195, 1999.

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

23. R.S. MACKAY, *Transition to chaos for area preserving maps*, in: Nonlinear Dynamics Aspects of Particle Acceleretors, J.M. JOWETT, M. MONTYH and S. TURNER (Eds.), Lecture Notes in Physics, 247, 390–454, Springer, Berlin 1986.

24. Y.V. NAZAROV, *Novel circuit of Andreev reflection*, Preprint cond-mat 9811155, Los Alamos 1998.

25. G. NICOLIS and I. PRIGOGINE, *Die Erforschung des Komplexen*, Piper, Munich 1987.

26. E. OTT, C. GREBOGI and J.A. YORKE, *Controlling chaos*, Physical Review Letters, **64**, 11, 1196–1199, 1990.

27. U. PARLITZ, L.O. CHUA, LJ. KOCAREV, K.S. HALLE and A. SHANG, *Transmission of digital signals by chaotic synchronization*, Int.J.Bifurc. & Chaos, **2**, 973–977, 1992.

28. L.M. PECORA, T.L. CAROLL, *Synchronization in chaotic systems*, Phys. Rev.Lett. **64**, 8, 821–824, 1990.

29. Y. POMEAU, *Intermittancy: a simple mechanism of continuous transition from order to chaos*, [In:] Bifurcation Phenomena in Mathematical Physics and Related Topics, 155, Reidel, 1980.

30. M. SHINBROT, *Entropy change and no-slip condition*, Arch.Rat.Mech.Anal., **67**, 351–363, 1978.

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

32. J. SCHNUTE and M. SHINBROT, *Kinetic theory and boundary conditions for fluids*, Can. J. Math.,. **25**, 1183, 1973.

33. I. SHIMADA and T. NAGASHIMA, *A numerical approach to ergodic problem of dissipative dynamical systems*, Progress Theor. Phys., **61**, 1605–1616, 1979.

34. J-M. STRELCYN, *The "coexistence problem" for conservative dynamical systems: A review*, Colloqium Mathematicum, **62**, 2, 331–345, 1991.

35. J. SZCZEPAŃSKI and Z. KOTULSKI, *On topologically equivalent ergodic and chaotic reflection laws leading to different types of particle's motion*, Arch.Mech, **50**, 5, 865–875, 1998.

36. J. SZCZEPAŃSKI and E. WAJNRYB, *Long-time behaviour of the one-particle distribution function for the Knudsen gas in a convex domain*, Physical Review A, **44**, 6, 3615–3621, 1991.

37. J. SZCZEPAŃSKI and E. WAJNRYB, *Do ergodic or chaotic properties of the reflection law imply ergodicity or chaotic behaviour of a particle's motion?*, Chaos, Solitons & Fractals, **5**, 1, 77–89, 1995.

Received December 30 1998; revised version March 18, 1999.