BIULETYN WAT
ROK XLVIII,
NR 10(566),
PP.111-123, 1999

On the application of discrete chaotic dynamical systems to cryptography. DCC method.

ZBIGNIEW KOTULSKI, JANUSZ SZCZEPAŃSKI

Polish Academy of Sciences, Institute of Fundamental Technological Research, PL-00-049 Warsaw, Świętokrzyska 21, Poland

Abstract. In the paper we present some methods of constructing cryptosystems utilising chaotic dynamical systems that has been extensively developed last years. We start with a brief review of algorithms based on both the theory of continuous and discrete systems. Then we show our approach where the essence of chaos (that is the sensitivity of the trajectories of discrete chaotic dynamical systems to the small changes of initial conditions) is exploited for secure communication.
Key Words: cryptosystems, chaos, dynamical systems
AMS subject classification (1991): 94A60, 58F13, 58F11

1. Introduction

Cryptography is as old as the need of sending confidential messages for long distances and protecting stored data. It usually uses modern branches of sciences, especially new mathematical results, and applies the recent technological achievements. We can even say that cryptography stimulates progress in these fields. Now, in time of computer global communication and mobile telephony there is a necessity of creating new, both fast and secure algorithms of encryption and decryption. In this paper we indicate a possibility of application of dynamical systems (continuous as well as discrete) for the purpose of secure communication.

As a starting point, we locate the place of the dynamical systems construction among other cryptographical algorithms. The cryptosystems can be classified with respect to the three following aspects:

1. Classification with respect to the structure of encryption algorithm.

   1a. Stream ciphers, where all the binary representation of the message is being encrypted bit after bit with application of a stream of random (pseudorandom) bits;

   1b. Block ciphers, where the binary representation of the message is divided into finite length blocks and being encrypted block after block with application of a bijective function depending of some parameter (the secret key);

2. Classification with respect to the method of distribution of the secret key. Here we have:

   2a. Private secret key cryptosystems;

   2b. Public key cryptosystems;

3. Classification with respect to the methods of constructing the algorithm.

   3a. Traditional methods using (see [16]):

      - number theory;
      - algebra;
      - algebraic geometry (recently: elliptic curves over finite fields [5]);
      - combinatorics;
      - research for the systems with large complexity;
      - development of hardware and software.

   3b. Methods utilising chaos

      - continuous dynamical systems;
      - discrete dynamical systems;

2. Applications of chaos in secure communication

Last years a new approach of constructing cryptosystems based on application of the theory of both continuous and discrete chaotic dynamical systems has been developed. In frames of continuous theory the methods of synchronisation of chaotic systems [4] and the idea of controlling chaos [4] [12] are applied. The discrete systems methods concentrate on iterations and inverse iterations of chaotic maps and possibilities of intelligent way of introducing keys.

The earliest applications of chaotic systems in cryptography were proposed by Pecora and Caroll in 1990 [15] as a possible application of the synchronisation of chaotic dynamical systems. This idea has been developed by Kocarev et al. [6] and Parlitz et al. [13], where they presented an experimental test system based on an chaotic electronic circuits. The first paper employed an analog signals while the second one used binary information model. The overview of the methods connected with encrypting messages with the modulation of trajectories of continuous dynamical systems can be found in [5].

Application of discrete chaotic dynamical systems to cryptography was first analysed by Habutsu et al. [3] and then developed by Kotulski and Szczepañski [8].

Continuous chaotic dynamical systems

Now we present briefly an idea of continuous chaotic cryptosystems. In these systems the message is being encrypted with the use of a continuous, chaotic dynamical system. Such a system is described by a system of non-linear ordinary differential equations and its qualitative behaviour (like chaos, ergodicity, etc.) depends on the values of internal parameters. If the system is chaotic, its trajectories are extremely sensitive to small changes of the initial conditions. The encryption procedure is based on the modulation of the system trajectories.

The first method of secure communication uses the procedures of so called synchronisation of chaotic trajectories. In this method the original message $I(t)$

(time-varying series of pulses) is masked by adding it to some larger chaotic signal $n(t)$. The receiver obtains $n(t)+I(t)$. The decryption is extracting the information from the obtained trajectory, that is the elimination of the chaotic noise. This is possible when the chaotic signal in the transmitter and receiver can be synchronised. As it is seen, in this approach the chaotic trajectory plays a role of the secret key. (This is an analogue of stream bit ciphers.) Practically, the receiver must know the internal parameters of the dynamical system generating the chaotic trajectory and the trajectory's initial condition.

The second construction of cryptosystem uses the methods of controlling chaos [11], [12]. Now the message is included in a specific way into the chaotic trajectory. The sender fixes the initial values of the internal parameters of the system equation and chooses the initial condition of the trajectory. The parameters and the initial condition must be such that the trajectory is chaotic. The chosen initial values of the internal parameters play a role of the secret key. The message must be transformed to the series of changes of the internal parameter (e.g. the initial value of the parameter plus-minus a small perturbation). Then the trajectory of the system is generated in such a way, that the internal parameter is modulated in constant time spacing according to the binary representation of the message. The receiver obtains the modulated trajectory (containing the encrypted message) and he knows the secret key (the initial value of the internal parameter). To decrypt the message he uses the same dynamical system and generates his own trajectory. Starting from the known initial condition and the initial value of the parameter he restores the original trajectory changing the value of the internal parameter using the controlling chaos method. This way he is able to register the jumps of the parameter and, what it follows, to decrypt the message. The security of the system is based on the property of strong sensitivity of the system to tiny perturbations of the parameter (the butterfly effect).

Let us remark that the construction of cryptosystem based on synchronisation of chaotic trajectories corresponds to external exciting of a dynamical system by some signal (message) while cryptosystems using controlling chaos method can be considered as a systems with internal (parametric) excitations.

Discrete chaotic dynamical systems

Another promising possibility is the application of discrete dynamical systems. This idea was suggested by T.Habutsu et al. [3]. The authors assumed some parameter of the „tent map" to be a secret key. Then the message (initial condition) was transformed by several inverse iterations of the map. This method works for the systems for which the map properties are strongly sensitive to small changes of the internal parameter playing the role of secret key. Trying to generalise this approach we face to the problem of finding if this property really takes places for certain dynamical systems. (Some weak points of this algorithm in the case of the tent map were presented in [2]). Therefore it is worthily to construct a cryptographic algorithm using the essence of chaos, i.e. exponential divergence of trajectories for different initial conditions.

Our idea is to introduce the secret key into the initial condition of the discrete chaotic system. In the papers [8], [9], [10] we proposed another method of constructing cryptosystems utilising discrete chaotic dynamical systems. During iteration, an initial condition of the chaotic dynamical system is being transformed in a very non-regular way. Therefore the encryption and decryption procedure is based on multiple n-th inverse iteration and n-th iteration of a certain two-dimensional chaotic system. We assume that one part of the initial condition is the message, the other one is the secret key. To ensure a complicated structure of trajectories of the dynamical system proposed as the algorithm, we postulate that except of being chaotic, the system should be ergodic or, preferably, mixing. These properties make that our cryptosystem is robust against any reasonable statistical attack and ensure the standard quality of the cryptosystem. The approach presented made it

possible to construct cryptosystems and verify their safety by the methods of the theory of abstract dynamical systems. Thus, we have a very strong tool available.

We introduce two classes of chaotic dynamical systems which we apply for preparation of cryptographic algorithms. The first class has its source in investigations of very rarefied gases, so called reflection law models [1], [17], [18]. In this case we assume that the key is introduced into the reflection law and the message is considered as the initial position of the particle. The second class is constructed in an abstract way. The map used for the encryption and decryption is some postulated function.

A brief overview of applications of chaos in secure communications is announced in the following table:

Continuous Dynamical Systems	**Discrete Dynamical Systems**
Encryption of a message with modulation of trajectories	Encryption of a plaintext with *n*-th inverse iteration of a map
Decryption of a ciphertext by synchronisation of two systems or reconstruction of the changes of internal parameters	Decryption of a ciphertext with *n*-th iteration of the map
Tools applied:	Tools applied:
- synchronisation of two chaotic systems	- chaos
- controlling chaos	- ergodic theory
T.Caroll, L.Chua, L.Doerner, K.Eckert, C.Grebogi, K.Halle, S.Hayes, B.Huebinger, L.Kocarev, W.Martienssen, E.Ott, U.Parlitz, L.Pecora, J.York	Two approaches: - including the secret key into internal parameter of the map T.Habutsu, Y,Nishio, I.Sasase, S.Mori EUROCRYPT'91 - including the secret key into initial conditions

Book:	Z.Kotulski, J.Szczepański K.Górski, A.Paszkiewicz,
T.Kapitaniak, *Controlling Chaos*	A.Zugaj

3. Description of DCC method

Now we formulate the method of application of chaotic dynamical systems for secure communication more precisely. For completeness let us remind the fundamental definition.

A discrete dynamical system [14] is the couple (X,φ), where X is the state space with some structure, (for our purpose: an interval or Cartesian product of two intervals) and φ is a transformation from X to X, called the generator of the semi-group of iterations.

The idea of Discrete Chaotic Cryptography

Plaintext is some number $P \in (0,\ 1)$;

Secret key is some parameter k;

Encryption is the n-fold iteration of the inverse map φ^{-1} with the initial value P according to some (secret) rule of choices of the successive pre-images of φ^{-1};

Ciphertext C is a result of the encryption:

$$C = \varphi^{-n}(P) = \varphi^{-1}\left(\varphi^{-1}\left(\ldots\varphi^{-1}(P)\right)\right);$$

Decryption is calculation of the image of C under the n-th iteration of the map φ:

$$P = \varphi^{n}(C) = \varphi\left(\varphi\left(\ldots\varphi(C)\right)\right).$$

The secret key k can be introduced to the algorithm in the following way:
into the initial condition [9]; $P := P_k$;

into internal parameters of φ [3]; $\varphi := \varphi_k$.

To make the encryption procedure very complicated we assume the chaos property of dynamical systems used.

Chaos is the property of sensitive dependence of trajectories from the initial conditions. More precisely, the non-linear system is chaotic if it has positive Lyapunov exponents on some domain.

As an example consider a one dimensional dynamical system (I, φ), where φ is C^1. If at a point $x \in I$, $\lambda_x > 0$ (Lyapunov exponent) then

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

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 $e^{(\lambda_x - \varepsilon)n}$ times.

Let us illustrate the idea of including the secret key into the initial condition by an elementary one-dimensional example.

An illustrative example

Let γ be a one-dimensional chaotic map with positive Lyapunov exponent λ:

$$\gamma : [0, 1] \to [0, 1]$$

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,

$$\overline{C} = \gamma^{-n}(P),$$

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

Then, we calculate C, the ciphertext of P as

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

Decryption is the inverse operation to γ^{-n}, that is

$$P=\gamma^n(C-k).$$

A non-legal user 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 $P_1=\gamma^n\left(C-k_1\right)$. For $n=30$, $\lambda-\varepsilon\approx 1.558$ (what is a reasonable value for many dynamical systems), due to chaos we have:

$$\left|P-P_1\right|=\left|\gamma^n(C-k)-\gamma^n\left(C-k_1\right)\right|\geq e^{n(\lambda-\varepsilon)}\left|k-k_1\right|\approx 0.5.$$

This shows how the chaos property preserves the system against the brute force attack (where the algorithm is tested with all possible secret keys).

However, cryptoanalysts use more sophisticated attacks to break cryptosystems. To make the cryptosystem based on the chaos property more robust against statistical cryptoanalitycal attacks, we postulate 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 Lebesgue measure.

Ergodic properties - notation

We say that the measure μ is <u>invariant</u>, if and only if it satisfies

$$\forall A\in\sigma(X),\quad \mu(A):=\mu\left(\varphi^{-1}(A)\right).$$

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

$$\forall A \in \sigma(X),\ \mu(A) = \int_A g(x)dx ,$$

with its density function

$$0 < g_1 \le g(x) \le g_2 ,$$

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 smaller region. It means that the plain-text space which can correspond to a given cipher cannot be restricted to a "smaller" subspace (smaller then *X*). Thus, for the cipher-text *C* the corresponding plain-text *P* (during brute attack) must be searched for over all the state space *X*.

The system is mixing if the following condition is satisfied (we assume that $\mu(X) = 1$):

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

This property means that the part of *B* that after *n* iterations of φ will be contained in *A* is asymptotically proportional to the rate of *A* in *X* with respect to the measure μ. Thus for any cipher-text *C* all the possible plain-texts *P* (during brute attack) are μ-equiprobable.

For more details about foundations of ergodic theory see [14].

Discrete Chaotic Cryptography - implementation 1

The idea of sensitive dependence on initial conditions (chaos) and ergodicity has its source in the theory of gases (*n*-particles models, Lorentz gas, Brownian motion). Therefore in the first cryptosystem we apply two-dimensional reflection law models [1], [17], [18]. This can be considered as an idealised model of a particle's movement in some environment (bounded domain). In the theory of gases 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 guar-

antees 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. Thus, 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 our cryptosystem, we take the initial condition of the first co-ordinate of the system (which describes the position of the particle on the boundary at the moment of reflection) as the plain-text and the initial condition of the second co-ordinate (representing the angle of reflection according to some reflection law) as the secret key. Both co-ordinates are iterated; the second, independently of the first (due to specific choice of the model), in a chaotic way; the first with some dependence on the second co-ordinate at each step. Under certain assumptions on the dynamical system, taking two initial conditions, we have an exponential divergence of their trajectories, depending on the distance of the initial conditions of both trajectories.

To precise our model we consider the motion of a free particle in a square. Describing it we use the co-ordinate system $\left(x_n, v_n\right)$, where x_n is the position of the particle at the boundary of the square at the moment of the *n*-th reflection and v_n is the angle from the tangent to the boundary at x_n to the direction of velocity of the particle after the reflection.

At the boundary the particle undergoes a reflection law:

$$T_D:(0,\pi)\to(0,\pi), \qquad T_D(v_{inc}) = v_{ref}$$

where v_{inc} is the angle of incidence and v_{ref} is the angle of reflection.

The movement of the particle is described by the following two-dimensional map

$$F_{T_D} : [0,\ L)\times(0,\ \pi) \longrightarrow [0,\ L)\times(0,\ \pi),$$

$$F_{T_D}\left(x_n, v_n\right) = \left(x_{n+1}, v_{n+1}\right).$$

Taking into account the geometry of the square, we come to the explicit formula:

$$F_{T_D}(P,k) = \left(S(P,k), T_D(k)\right).$$

In this model we take the initial value v_0 as a secret key:

$$k \equiv v_0 \ .$$

We see that the evolution of the second co-ordinate describes the evolution of the secret key.

To obtain the appropriate properties of the extended system F_{T_D} we put some conditions on the reflection law T_D.

Conditions on the reflection law

1. $T_D:(0,\ \pi) \to (0,\ \pi)$;

2. The interval $(0,\ \pi)$ can be divided into finite (or infinite countable) number of intervals $\Delta_1, \Delta_2, \ldots$ such that

$$T_D(\Delta_i) = (0,\ \pi), \qquad i = 1,2,\ldots;$$

3. At each Δ_i the map T_D is of class C^2 and monotonic;

4. For some natural *s* and every *i* the following relationship is satisfied

$$\inf_{\Delta_i} \inf_{k \in \Delta_i} \left| \frac{dT_D^{(s)}(k)}{dk} \right| = \delta > 1,$$

where $T_D^{(s)}$ is the *s*-th iteration of the map T_D;

5. $$\sup_{\Delta_i} \sup_{k_1, k_2 \in \Delta_i} \frac{\left| \frac{d^2 T_D(k_1)}{d k_1^2} \right|}{\left[\frac{d T_D(k_2)}{d k_2} \right]^2} = \rho < \infty .$$

Under the above conditions the map T_D is mixing and chaotic [7]. Proceeding the inverse iterations and also closing the procedure with adequate maps (composition of non-linear map with an interval exchange transformation) we obtain that chaos (mixing, ergodicity) is transferred to the extended system F_{T_D}.

The next example of DDC system is constructed in some abstract way.

Discrete Chaotic Cryptography - implementation 2.

In the following cryptosystem we propose the algorithm using some abstract dynamical system. In the system the part decrypting a given ciphertext can be considered, in some sense, as a multiplicative perturbation of the chaotic dynamical system transforming the secret key.

More precisely, we construct a two-dimensional dynamical system (X, Φ) where X is the Cartesian product of two unit intervals and Φ is the map:

$$\Phi : [0, 1]\times[0, 1]\rightarrow [0, 1]\times[0, 1],$$

of the following form

$$\Phi(k, C) = [\phi(k), \chi(C, k)\phi(k)].$$

We interpret the first argument of Φ as the secret key and the second argument as the cipher-text. We assume that $\phi:[0,1]\rightarrow[0,1]$ is a chaotic and mixing map and χ is a transformation satisfying some special conditions [9]. To complete the model we apply in the encryption procedure a concentrating map proceeding the inverse iterations and also close the procedure with adequate spreading map. Under the above assumptions, in this system we have transferring of chaos (and also ergodicity and mixing property) from the subsystem ϕ to the whole system Φ. Thus we obtain the secure tool for encrypting the messages. The details of the model can be found in [9].

4. Prospects and perspectives

In the paper we present a general method of constructing cryptosystems with application of discrete chaotic dynamical systems by utilisation of the essence of chaos (i.e. the sensitivity of the trajectories to small changes of initial conditions). Our approach made it possible to construct cryptosystems and verify their safety by methods of the theory of abstract dynamical systems [14]. Since the theory is well developed and still extensively investigated, we have a very strong tool available.

A general theory of discrete chaotic cryptosystems is a kind of theoretical model. In practice, preparing concrete computer implementations, one should take into account the usual computational conditions. Since numbers in numerical computations have finite representation, one must assume a size of computed values (key, plaintext, ciphertext) such that both the iterations and inverse iterations can be performed uniquely and such that one can obtain the required number of significant digits of plaintext in the decryption process. This property depends on the dynamical model, the algorithm applied for calculation of required maps and com-

puter used in concrete implementation. Let us remark that the proposed algorithm is very fast in comparison to other known block ciphers. It requires only n iterations of some relatively simple maps, where the number n must be some compromise between safety of the method and accuracy of the computer arithmetic. Usually $20 \le n \le 100$ [10].

It is an obvious fact that hardware improvement will continue inexorably. Using more modern equipment we can deal with longer computer words and, what it follows, work on a richer state space. This makes the numerical model closer to theoretical chaotic one, which, by theory, is completely secure. Finally, it is important to realise that hardware improvement make cryptosystems more secure, not less. This is because a hardware improvement that allows an attacker to use a number of two digits longer than before will at the same time allow a legitimate user to use a key dozens of digits longer than before; a user can choose a new key a dozen digits longer than the old one without any performance slowdown. Thus although the hardware improvement does help the attacker, it helps the legitimate user much more.

Some results of this paper have been presented at the conference NEEDS'97, Crete [9].

REFERENCES

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

[2] BIHAM E., *Cryptoanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91*, EUROCRYPT'91, pp.532-534.

[3] HABUTSU T., NISHIO Y., SASASE I., MORI S., *A secret key cryptosystem by iterating a chaotic map*, EUROCRYPT'91, pp.127-136.

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

[5] KOBLITZ N., *A course in Number Theory and Cryptography*, Springer-Verlag, Berlin 1994.

[6] KOCAREV LJ., HALLE K.S., ECKERT K., CHUA L.O., PARLITZ U., *Experimental demonstration of secure communications via chaos synchronization*, Int.J.Bifurc. & Chaos **2** (1992), 709-716.

[7] KOSJAKIN A.A., SANDLER E.A., *Ergodic properties of some class of piecevise smooth maps on the interval*, Matiematika **3** (1972), 32-40.

[8] KOTULSKI Z., SZCZEPAŃSKI J., *Discrete chaotic cryptography*, Annalen der Physik **6** (1997), 381-394.

[9] KOTULSKI Z., SZCZEPAŃSKI J., *Discrete chaotic cryptography. New method for secure communication*, Proceedings of Nonlinear Evolution Equations and Dynamical Systems 1997, Crete, http://www.roma1.infn.it/ ~ragnisco /proc97.htm.

[10] KOTULSKI Z., SZCZEPAŃSKI J., GÓRSKI K., PASZKIEWICZ A., ZUGAJ A., *Application of discrete chaotic dynamical systems in cryptography - DCC method.* Vol.9, No.6, pp.1121-1135 (1999).

[11] MARTIENSSEN W., HÜBINGER B., DOERNER R., *Chaotic cryptology*, Annalen der Physik **4** (1995), 35-42.

[12] OTT E., GREBOGI C., YORKE I.A., *Controlling chaos*, Phys.Rev.Lett. **64** (1990), 1196-1199.

[13] PARLITZ U., CHUA L.O., KOCAREV LJ., HALLE K.S., SHANG A., *Transmission of digital signals by chaotic synchronization*, Int.J.Bifurc. & Chaos **2** (1992), 973-977.

[14] PARRY W., *Topics in Ergodic Theory*, Cambridge Univ. Press, Cambridge 1981.

[15] PECORA L.M., CAROLL T.L., *Synchronization in chaotic systems*, Phys.Rev.Lett. **64** (1990), 821-824.

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

[17] SZCZEPAŃSKI J., KOTULSKI Z., *On topologically equivalent ergodic and chaotic reflection laws leading to different types of particle motion*, Archieves of Mechanics **50** (1998), 865-875.

[18] SZCZEPAŃSKI J., WAJNRYB E., *Do ergodic or chaotic properties of the reflection law imply ergodicity or chaotic behaviour of a particle's motion?*, Chaos, Solitons & Fractals **5** (1995), 77-89.

Z.KOTULSKI, J.SZCZEPAŃSKI

Zastosowanie dyskretnych chaotycznych układów dynamicznych w kryptografii. Metoda DCC

Praca poświęcona jest omówieniu metod intensywnie rozwijanych w ostatnich latach, dotyczących konstruowania kryptosystemów wykorzystujących teorię chaotycznych układów dynamicznych. W zwięzły sposób przedstawiono w niej najnowsze algorytmy tego typu oparte zarówno na ciągłych jak też na dyskretnych układach dynamicznych. Następnie zaprezentowano własne podejście do tego zagadnienia, w którym podstawą algorytmu jest teoria dyskretnych układów chaotycznych. Jego istotą jest silne uwzględnienie w algorytmie najważniejszej własności trajektorii chaotycznych, to znaczy ich wykładniczej wrażliwości na małe zmiany warunków początkowych.