Institute of Physics Publishing Journal of Physics: Conference Series **23** (2005) 210–214
doi:10.1088/1742-6596/23/1/023 International Conference on Control and Synchronzation of Dynamical Systems

Information safety by suppression of chaos

A.Loskutov and A.A.Churaev

Physics Faculty, Moscow State University, Moscow 119899, Russia

E-mail: newchuraev@yandex.ru

Abstract. A new original method of information processing and secure communications based on the coding of alphabet symbols by stabilized cycles of certain perturbed one-dimensional dynamical systems is proposed. The foundation of the proposed method is ciphering by the one-to-one correspondence between periods of such cycles and certain alphabet symbols. It is shown that for some maps perturbations which lead to the stabilization of cycles of the given period, form some domain in the parametric space. This fact is used for coding identical symbols via random selection of parameters from this domain, that ensures that the probability of decoding the transmitting information by an external observer is zero. Analytic estimations of the admissible noise level in the communication channel and the randomness degree of transmitting signals are made. Some variants of the ciphered sequences are presented.

1. Introduction

In the present stage of the development of communication technologies, the problem of protecting information is most important. We propose an original method of data encoding, which makes use of the possibility of stabilizing the cycles of chaotic maps. This possibility is based on the well known fact form the theory of dynamical systems [1, 2, 3] (see also [4, 5] and references therein): there exist periodic perturbations of the chaotic dynamical systems belonging to general types, which lead to stabilization of the cycle with a given period. Although data encoding by means of chaotic systems is now very popular (see, e.g., [6, 7, 8, 9, 10, 11] and references therein), the proposed method is advantageous in allowing a network application to be developed for exchanging messages without preliminary synchronization of the transmitter and receiver (which is usually necessary in other approaches). Moreover, programs to be developed in the nearest future will allow sound messages to be encoded as well.

We develop an analytic approach to a parametric (multiplicative) non-feedback method of the stabilization of the prescribed orbits of dynamical systems. In the contrast to the well-known methods of the feedback controlling the behavior, the described rigorous results look more suitable for applications because they does not require a real-time computer analysis of the state of the system, and it is more robust to noise. On the basis of the theory we develop a new original method for secure communications. The basis of this method is a one-to-one correspondence between periods of stabilized cycles and certain alphabet symbols. As a transmitted signal, the corresponding periodic perturbations are used, and a key for the decoding of the received signal is a form of the dynamical system (i.e. the function describing this system).

2. Stabilization of cycles

In order to explain the proposed principle of data encoding, we will first describe the main theoretical result concerning the stabilization of cycles. Consider a map of some region M and $\mathbf{R}^j$ into itself:

$$T_a : \mathbf{x} \longmapsto \mathbf{f}(\mathbf{x}, a) \ , \tag{1}$$

where a is a parameters from the manifold of possible values $A \subset \mathbf{R}$, $\mathbf{x} = \{x_1, \ldots, x_j\}$ and $\mathbf{f} = \{f_1, \ldots, f_j\}$. Let us introduce the concept of parametric perturbation. The most natural way of doing this is to define a map with respect to parameter a , which would determine its value at each moment of time, $G : A \to A$, $a \to q(a)$. A perturbation will be called periodic with a period of τ, provided that the function $g(a)$ is defined only in τ points $a_1, \ldots, a_\tau$ in the following manner: $a_{i+1} = g(a_i), i = 1, \ldots, \tau - 1$ and $a_1 = g(a_\tau)$.

In this case, the set of perturbations with period τ can be brought into correspondence with manifold $\mathbf{A} = \{\hat{a} \in \underbrace{A \otimes A \otimes \cdots \otimes A}_{\tau \text{ times}} : \ \hat{a} = (a_1, \ldots, a_\tau), \ a_i \neq a_j, \ 1 \leq i, j \leq \tau, \ i \neq j,$ $a_1, \ldots, a_\tau \in A\}$, $\mathbf{A} \subset \mathbf{R}^\tau$. Let us introduce a submanifold $A_c \subset A$ corresponding to only the chaotic behavior of map (1). In some papers (see, e.g., [2, 12, 13, 14, 15]), it was proved that, for $j = 1$ and $j = 2$, there exist perturbations $\hat{a} = (a_1, a_2, ..., a_\tau)$ such that, for $\hat{a} \in \mathbf{A}_c$ (or $g(a) \in A_c$), a perturbed map will be regular with a stable cycle of period $t = \tau n$. Moreover, the following exact result is valid for onedimensional maps ($j = 1$) [5].

Let a map $T_a : x \longmapsto f(x, a)$, $x \in M$, $a \in A$ to obey the conditions: (i) there exists a submanifold $\sigma \subset M$ such that, for any $x_1, x_2 \in \sigma$, there can be found $a^* \in A$ for which $f(x_1, a^*) = x_2$ and (ii) there exists a critical point $x_c \in \sigma$ such that $\partial f(x, a)/\partial x|_{x=x_c} \equiv D_x f(x_c, a) = 0$ for any $a \in A$. Then, for any $x_2, x_3, ..., x_\tau \in \sigma$, there can be found x_1 and $a_1, a_2, ..., a_\tau$ such that the cycle $(x_1, x_2, ..., x_\tau)$ will be a stable cycle of perturbed map T_a for $\hat{a} = (a_1, a_2, ..., a_\tau)$.

3. The encoding method

For data encoding, it is necessary to develop a method for evaluating the permissible noise level (see [15]). This can be readily done as follows [5]. Let the perturbed map T_a for $\hat{a} = (a_1, a_2, ..., a_\tau)$ to have a stable cycle of period τ, $p = (x_1, x_2, ..., x_\tau)$. Then, provided that

$$|\Delta a_i| \leq \delta_a = 1 \Big/ \left(\tau A_a L S_x^{\tau-1} \sum_{i=1}^{\tau} S_x^i \right),$$

where $i = 1, 2, \ldots, \tau$; $S_a = |D_a f(x, a)|$; $L = \max\limits_{x,a} |D_x^2 f(x, a)|$; and $S_x = \max\limits_{x,a} |D_x f(x, a)|$. This map also has a stable cycle, $p' = (x_1 + \Delta x_1, x_2 + \Delta x_2, \ldots, x_\tau + \Delta x_\tau)$ of period τ for $\hat{a}' = (a_1 + \Delta a_1, a_2 + \Delta a_2, \ldots, a_\tau + \Delta a_\tau)$, where $|\Delta x_i| \leq \delta_x = 1 \Big/ L S_x^{\tau-1}$.

In the first step of encoding, it is necessary to obtain the ASCII codes of all symbols involved in the text to be encoded. As is known, each symbol in the ASCII system corresponds to a unique triad of integers. For example, Latin letter a corresponds to the ASCII code 97 with the triad $n_1 = 0, n_2 = 9, n_3 = 7$. Then, each member of a triad is interpreted as the period of a cycle inherent in a dynamical system. In order to avoid degenerate cycles (period 0) and stable cycles (period 1), we add 2 to each n_i $(i = 1, 2, 3)$. Now, using the chaotic properties of an applied map (or the random number generator), we create a sequence with a length equal to the sum of all n_i (increased by 2) plus 1. The last element is used for beginning the count of cycle periods.

The obtained sequence of random numbers is considered as the sequence of values of the dynamical variable x. For this sequence to bear information concerning the encoded symbols, we replace a part of elements by the values of critical points x_c, that is, the points where $f'(a, x)|_{x_c} = 0$. These points are separated by $n_i + 2$ steps beginning with the first. Thus, the sequence consists of subsequences, the number of which is equal to the number of members in

the sequence $(n_i + 2)$, that is, to the number of symbols in the coded text multiplied by three. The periods of cycle will be equal to $n_i + 2$.

Now let us calculate the values of the control parameter $\hat{a} = a_1, \ldots, a_n$, that is, determine the perturbation stabilizing the obtained sequence of cycles. This can be readily done by considering the inverse problem of determining the parameters from the form of the map. For particular maps, perturbations $\hat{a}$ producing stabilization of the cycle of a given period form a certain region in the parametric space. This circumstance can be used for encoding repeated symbols by means of random selection of parameters from this region.

The main steps of the data encoding protocol using the proposed method are presented in Table 1. The final sequence $a_1, \ldots, c_{n_3+2}$ (representing parameters rather than the message) is sent to a transmitter, where all operations (with certain differences related to rounding) are performed in the reverse order (the method is symmetric).

Table 1. The principle of encoding symbols and letter sequences for secure data transmission

$$\left\{ \begin{array}{c} \mathbf{Y} \\ symbol \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \mathbf{n_1},\ \mathbf{n_2},\ \mathbf{n_3} \\ ASCII - codes \end{array} \right\} \longrightarrow$$

$$\longrightarrow \left\{ \begin{array}{c} \{\mathbf{a_1}, \ldots, \mathbf{a_{n_1+2}}\}, \{\mathbf{b_1}, \ldots, \mathbf{b_{n_2+2}}\}, \{\mathbf{c_1}, \ldots, \mathbf{c_{n_3+2}}\} \\ sets\ \ of\ \ parameters \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \mathbf{a_1}, \ldots, \mathbf{c_{n_3+2}} \\ seq.\ of\ numbers \end{array} \right\}$$

4. Justifications

In order to justify the proposed method, it is necessary to perform a statistical correlation analysis and evaluate the cryptographic stability [16]. The statistical analysis was performed using a sequence of 900 values of the control parameters, encoding a message consisting of 1000 Latin letter o symbols. The transmission of this symbol represents the most dangerous regime of operation of the proposed method, since the ASCII code of this symbol is 111 and the information about each o is contained in the three sequential cycles of period $n_i + 2 = 1 + 2 = 3$, whose repetition is highly undesired. Satisfactory results obtained in this particular case will provide evidence of even greater reliability of the proposed method in the case of encoding other symbols. The statistical analysis gave the following results: correlation coefficient, $r = 0.0077$; regression equation, $y = 4.9322905 + 0.00769911509x$; the average value in the set, $\overline{x} = 4.96478169$. Therefore, the proposed method of data encoding is highly reliable from the standpoint of correlation analysis and is capable of protecting data messages of considerable length.

The main qualitative measures of cryptographic stability of an encrypting system are the laboriousness and reliability of the cryptographic analysis [17, 18]. We have evaluated the cryptographic stability of the proposed data encoding protocol by method of total probing, which consists in sequential random and equiprobable trial of N keys without repeats from manifold K.

Table 2. Results of evaluation of the laboriousness of decoding.

Byte/coefficient	$\lvert K\rvert$	$E^{\alpha,\beta}$	$t_{(\lvert E\rvert)}$
1	2^{27}	2^{26}	67 s
2	2^{51}	2^{50}	30 years
3	2^{75}	2^{74}	$6 * 10^8$ years
4	2^{99}	2^{98}	10^{16} years
5	2^{123}	2^{122}	$1,5 * 10^{23}$ years

Note: the left column indicates the number of bytes intended for encoding the control parameter; the right column shows the laboriousness of decoding converted into time assuming the computation speed to be equal to that of modern supercomputers.

The process of probing is terminated upon testing k keys, where $k = j$, $1 < j < N$, j being the first key number for which the decoded text is considered substantially meaningful, or $k = N$ if this event does not take place for $j \leq N$. The decoded text is assessed for meaningfulness using the following hypotheses: $H(0)$ for the open text and $H(1)$ for a random text. In formulating a probabilistic model, the assessment procedure is characterized by the following errors: $\alpha = P(H(1)/H(0))$, the probability of rejecting a meaningful text, and $\beta = P(H(0)/H(1))$, the probability of taking a meaningless text as meaningful. A model for calculation of the laboriousness of the cryptographic analysis can be formulated as

$$E^{\alpha,\beta}(|K|) = \frac{1}{|K|}\sum_{k=1}^{r} k(1-\beta)^{k-1}[\beta(r-k) + \frac{\alpha\beta}{1-\beta}(k-1) + (1-\alpha)] + \frac{r}{|K|}r\alpha(1-\beta)^{r-1} +$$

$$+\frac{|K|-r}{|K|}(\sum_{k=1}^{r} k(1-\beta)^{k-1}\beta + r(1-\beta)^{r})$$

where $E^{\alpha,\beta}(|K|)$ is the mathematical expectation characterizing termination of the probing process after probing k keys and N is the number of probed keys. The results of calculations performed assuming errorless mechanism of taking decisions ($\alpha = 0$, $\beta = 0$) are summarized in Table 2. The reliability was evaluated using the relation

$$P(r,\alpha,\beta) = \frac{1-\alpha}{|K|}\sum_{t=1}^{r}(1-\beta)^{t-1}$$

Obviously, reliability of the method of total probing assuming errorless mechanism of taking decisions (α= 0, β= 0) is $P = 1$.

5. Comparison with the other methods

For the comparison analysis we used the following methods: RSA, DES [17, 18]. RSA is a cryptographic system with an open key. Its main advantage is a high level strength, but RSA has also the weakness: low productiveness. DES (Data Encryption Standard) is much more fast method (in some cases $\sim 10^4$ order). DES is a block encryption method developed by IBM and US Government used as a standard ANSI (American National Standard Institute). Its advantage is the high productiveness. At the same time it has a grave disadvantage: a low system safety. Thus, using this methods it is necessary to change very often the key.

The expected productiveness of the hardware of the proposed method (based on the stabilized cycles) is $10 - 60$Kb/s that is almost the same as for the productiveness of DES. The middle length key for our method is 100b, that is also comparable with DES. In addition, this method is symmetrical with respect to the key (i.e. data is coding and decoding by one and the same key). DES is also symmetrical method, but RSA is asymmetric one (that is, for the decoding the other key is used). That is the reason why it is difficult correctly to compare by this way, because the analysis of the cryptostability is different for symmetric and asymmetric methods. In the other words, qualitative and quantitative estimations of symmetric and asymmetric methods, strictly speaking, is not equivalent. However, it is accepted as correct that the symmetric cryptographic method are more safe.

If our theoretical analysis will be verified in practice (to this end it is necessary to make a deep and careful expertise) then this methods can be considered as a competitive product. Among forward-looking applications we may propose audio encryption (say, in the mobile devices), electronic digital signatures and safety of messages sending by e-mail.

6. Conclusion

In the present paper, a new original method of information processing and secure communications by stabilizing prescribed orbits of one-dimensional dynamical systems is proposed. Using in applications some family of polymodal maps, one can develop a quite efficient scenario for the search of perturbations which lead to the stabilization of orbits passing through the *given* points. In this case it is easy to automatize the coding, transmission and decoding procedures, that is an essential merit of the described method.

This scenario is realized by IBM-PC computer on the example of quadratic family maps. The main advantages of the proposed method are the following.

1. For its realization one can use a sufficiently large class of dynamical systems.

2. During communication the information sequence is not translated. Only signals which are necessary for the further information processing are sent.

3. Transmitting signal has a purely random character, that give a high level of the security.

4. Decoding is realized without predetermined synchronization of the transmitter and the receiver.

5. The method is stable with respect to an external noise.

6. Theoretically, the number of variants of the coding of one and the same transmitting sequence is infinite.

7. For every concrete application it is possible to estimate the admissible noise level in the communication channel.

Thus, points 2, 3, 4 provide a quite high security of the communication; points 1, 5, 6, 7 give a considerable opportunity in applications.

Because the proposed method is based on the rigorous mathematics, it is quite possible to construct some device for real secure communication. It can be produced in the two following forms. (A) As a software for some system for secure communication; (B) As an analog system with certain properties. For example, this can be a radio physical circuit with nonlinear (active) elements. But this is the subject of the further investigations.

7. References

[1] V.V.Alekseev and A.Loskutov 1987. Control of a system with a strange attractor through periodic parametric perturbation.— *Sov. Phys.-Dokl.*, v.32, No6, p.270–271.

[2] A. Yu. Loskutov and A. I. Shishmarev, — *Usp. Mat. Nauk* 48, 169 (1993).

[3] S.Hayes, C.Grebogi, E.Ott and A.Mark. Experimental control of chaos for communication.— *Phys. Rev. Lett.*, 1994, v.73, No13, p.1781–1784.

[4] S. Boccaletti, C. Grebogi, Y.-C. Lai, et al., — *Phys. Rev.* 329, 103 (2000).

[5] A. Loskutov, Mat. Model. 12, 314 (2001).

[6] K.M.Coumo, A.V.Oppenheim and S.H.Strogatz. Robustness and signal recovery in a synchronized chaotic system. — *Int. J. Bif. and Chaos*, 1993, v.3, No6, p.1629–1638.

[7] S. Hayes, C. Grebogi, E. Ott, and A. Mark. — *Phys. Rev. Lett.*, 73, 1781 (1994).

[8] L. Kocarev and U. Parlitz, — *Phys. Rev. Lett.* , 74, 5028 (1995).

[9] T. L. Carroll and L. M. Pecora, — *Chaos*, 9, 445 (1999).

[10] M. P.Kennedy and G. Kolumbn, — *Signal Process.*, 80, 1307 (2000).

[11] B. Fraser, P. Yu, and T. Lookman, — *Phys. Rev.*, E 66, 017 202 (2002).

[12] A.Loskutov and A.I.Shishmarev. Control of dynamical systems behavior by parametric perturbations: an analytic approach.— *Chaos*, 1994, v.4, No2, p.351-355.

[13] A. N. Deryugin, A. Yu. Loskutov, and V. M. Tereshko, — *Teor. Mat. Fiz.*, 104, 507 (1995).

[14] A.N.Derjugin, A.Loskutov and V.M.Tereshko. Inducing stable periodic dynamics by parametric perturbations.— *Fractals, Solitons, and Chaos*, 1996, v.7, No10, p.1-13.

[15] M. Dolnik and E. M. Bollt, — *Chaos*, 8, 702 (1998).

[16] Contemporary Cryptology: The Science of Information Integrity, Ed. by G. J. Simmons —IEEE Press, New York, 1992.

[17] Theory and Practice of Providing the Information Security, Ed. by P. D. Zegzhda — *Yakhtsmen, Moscow*, 1996.

[18] Cryptography, Ed. by V. P. Sherstyuk and E. A. Primenko — *SOLON-R, Moscow*, 2002.