Technical Physics Letters, Vol. 30, No. 10, 2004, pp. 843–845. Translated from Pis'ma v Zhurnal Tekhnicheskoĭ Fiziki, Vol. 30, No. 20, 2004, pp. 1–7.

Data Encoding by Stabilization of Dynamical System Cycles

A. Yu. Loskutov*, S. D. Rybalko, and A. A. Churaev

Moscow State University, Moscow, 119899 Russia
Bauman State Technical University, Moscow, 107005 Russia
** e-mail: Loskutov@moldyn.phys.msu.ru*

Received April 1, 2004

Abstract—A new method is proposed for masking transferred data with the aid of chaotic maps. The cryptographic stability is analyzed by the method of total probing. A correlation analysis of the obtained codes is performed and predictability of the code sequence is evaluated. A network application is developed, which allows legal users exchange messages protected by the proposed method. © *2004 MAIK "Nauka/Interperiodica".*

In the present-day stage of development of the communication technologies, the problem of protecting information is among most important. In this Letter, 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 of the theory of dynamical systems [1–3] (see also [4, 5] and references therein): there exist periodic perturbations of the chaotic dynamical systems belonging to rather 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., [6–11] 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.

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:

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

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, $G : A \longrightarrow A$, $a \longrightarrow g(a)$. 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 $A = \{\hat{a} \in \underbrace{A \otimes A \otimes \ldots \otimes A}_{\tau @}$:

$$\hat{a} = (a_1, \ldots, a_\tau),\ a_i \neq a_j,\ 1 \leq i, j \leq \tau,\ i \neq j,\ a_1, \ldots, a_\tau \in A\},$$

$$\mathbf{A} \subset \mathbf{R}^\tau$$

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, 12–12]), it was proved that, for $j = 1$ and $j = 2$, there exist perturbations $\hat{a} = (a_1, a_2, \ldots, a_\tau)$ 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 one-dimensional maps ($j = 1$) [5].

Let a map $T_a : x \mapsto f(x, a)$, $x \in M$, $a \in A$ 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 $x_2, x_3, \ldots, x_\tau \in \sigma$, there can be found x_1 and $a_1, a_2, \ldots, a_\tau$ such that the cycle $(x_1, x_2, \ldots, x_\tau)$ will be a stable cycle of perturbed map $\mathbf{T}_a$ for $\hat{a} = (a_1, \ldots, a_\tau)$.

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 $\mathbf{T}_a$ for $\hat{a} = (a_1, a_2, \ldots, a_\tau)$ to have a stable cycle of period τ, $p = (x_1, x_2, \ldots, x_\tau)$. Then, provided that

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

1063-7850/04/3010-0843$26.00 © 2004 MAIK "Nauka/Interperiodica"

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

$$\left\{\begin{array}{c} Y \\ \text{Symbol} \end{array}\right\} \longrightarrow \left\{\begin{array}{c} n_1, n_2, n_3 \\ \text{ASCII codes} \end{array}\right\}$$

$$\longrightarrow \left\{\begin{array}{c} \text{Cycles of periods } n_i + 2 \\ | \qquad\qquad | \\ x_0, \ldots, x_{n_1+2}, \ldots, x_{(n_1+2)+n_2+2}, \ldots, x_{(n_1+2+n_2+2)+n_3+2} \\ \text{Manifold of dynamical variables} \end{array}\right\}$$

$$\longrightarrow \left\{\begin{array}{c} \{a_1, \ldots, a_{n_1+2}\}, \{b_1, \ldots, b_{n_2+2}\}, \{c_1, \ldots, c_{n_3+2}\} \\ \text{Manifold of parameters} \end{array}\right\} \longrightarrow \left\{\begin{array}{c} a_1, \ldots, c_{n_3+2} \\ \text{Sequence of numbers} \end{array}\right\}$$

(where $i = 1, 2, \ldots, \tau$; $S_a = \max\limits_{x,\,a}|D_a f(x, a)|$; $L = \max\limits_{x,\,a}|D_x^2 f(x, a)|$; 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 $|\Delta x_i| \le \delta_x = 1/LS_x^{\tau-1}$.

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).

In order to justify the proposed method, iut 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, $\bar{x} = 4.96478169$. 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	K	$E^{\alpha, \beta}$	$t_{(E)}$
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 $j \le N$. 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

$$\mathrm{E}^{\alpha, \beta}(k) = \frac{1}{K}\sum_{k=1}^{N} k(1-\beta)^{k-1}$$

$$\times\left[\beta(N-k) + \frac{\alpha\beta}{1-\beta}(k-1) + (1-\alpha)\right] + \frac{N}{K}N\alpha(1-\beta)^{N-1}$$

$$+ \frac{K-N}{K}\left(\sum_{k=1}^{N} k(1-\beta)^{k-1}\beta + N(1-\beta)^{N}\right),$$

where $\mathrm{E}^{\alpha, \beta}(k)$ 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

$$P(N, \alpha, \beta) = [(1-\alpha)/K]\sum_{t=1}^{N}(1-\beta)^{t-1}.$$

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

Thus, the main advantages of the proposed method of data encoding are as follows: (i) the protocol can be implemented using a rather wide class of maps; (ii) the transmitted signal contains only information necessary for the further data processing, rather than the informative message as such; (iii) the dynamical system, which serves as the key for decoding, possesses chaotic properties; (iv) decoding process does not require preliminary synchronization of the transmitter and receiver; (v) the method is stable with respect to external noise; (vi) theoretically, the number of possible variants is infinite. As for practical realization, a network application has been developed, which allows legal users exchange messages protected by the proposed method.

REFERENCES

1. V. V. Alekseev and A. Yu. Loskutov, Dokl. Akad. Nauk SSSR **293**, 1346 (1987) [Sov. Phys. Dokl. **32**, 270 (1987)].
2. A. Yu. Loskutov and A. I. Shishmarev, Usp. Mat. Nauk **48**, 169 (1993).
3. E. Ott, C. Grebogi, and J. A. Yorke, Phys. Rev. Lett. **64**, 1196 (1990).
4. S. Boccaletti, C. Grebogi, Y.-C. Lai, *et al.*, Phys. Rev. **329**, 103 (2000). [Please, check this reference]
5. A. Loskutov, Mat. Model. **12**, 314 (2001).
6. K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).
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. Kolumbán, 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, Chaos **4**, 391 (1994).
13. A. N. Deryugin, A. Yu. Loskutov, and V. M. Tereshko, Teor. Mat. Fiz. **104**, 507 (1995).
14. A. N. Deryugin, A. Loskutov, and V. M. Tereshko, Chaos, Solitons and Fractals **7** (10), 1 (1996).
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).

Translated by P. Pozdeev

SPELL: 1. iut