09

Система кодирования информации посредством стабилизации циклов динамических систем

© А.Ю. Лоскутов, С.Д. Рыбалко, А.А. Чураев

Московский государственный университет им. М.В. Ломоносова
E-mail: Loskutov@moldyn.phys.msu.ru
Московский государственный технический университет им. Н.Э. Баумана

Поступило в Редакцию 1 апреля 2004 г.

Предложен новый метод защиты передаваемой информации посредством использования хаотических отображений. Проведен анализ криптостойкости методом тотального опробования, корреляционный анализ получаемых кодов и получена оценка предсказуемости значений кодовой последовательности. Разработано сетевое приложение, позволяющее пользователям обмениваться текстовыми сообщениями, защищенными представляемым методом.

На современном этапе развития информационных технологий проблема защиты информации чрезвычайно важна. В работе предложен оригинальный метод кодирования, основанный на возможности стабилизации циклов хаотических отображений. Он базируется на известном факте из теории динамических систем [1–3] (см. также [4,5] и цитируемую там литературу): для достаточно общих семейств хаотических динамических систем существуют периодические возмущения, приводящие к стабилизации цикла заданного периода. Хотя кодирование посредством хаотических систем сейчас весьма популярно (см., например, [6–11] и приводимые там ссылки), данный метод дает возможность развить сетевое приложение и обмениваться пользователям сообщениями, причем не требуется, как это обычно необходимо

при использовании подобных подходов, синхронизации передатчика и приемника. Более того, в ближайшем будущем планируется разработать программы, позволяющие кодировать и звуковые сообщения.

Для пояснения принципа кодирования опишем сначала основной результат, касающийся стабилизации циклов. Рассмотрим преобразование некоторой области M и $\mathbf{R}^j$ в себя:

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

где a — параметр из множества допустимых значений $A \subset \mathbf{R}$, $\mathbf{x} = \{x_1, \ldots, x_j\}$ и $\mathbf{f} = \{f_1, \ldots, f_j\}$. Введем понятие параметрического возмущения. Самым естественным способом является задание отображения по параметру, которое определяло бы его значение в каждый момент времени, $G : A \to A$, $a \to g(a)$. Возмущение назовем периодическим с периодом τ, если функция $g(a)$ определена только в τ точках $a_1, \ldots, a_\tau$ следующим образом: $a_{i+1} = g(a_i)$, $i = 1, \ldots, \tau - 1$ и $a_1 = g(a_\tau)$. В этом случае совокупность возмущений периода τ может быть поставлена в соответствие множеству $\mathbf{A} = \{\hat{a} \in \underbrace{A \otimes A \otimes \cdots \otimes A}_{\tau \text{ раз}}$: $\hat{a} = (a_1, \ldots, a_\tau)$, $a_i \neq a_j$, $1 \leqslant i, j \leqslant \tau$, $i \neq j$, $a_1, \ldots, a_\tau \in A\}$, $\mathbf{A} \subset \mathbf{R}^\tau$.

Введем подмножество $A_c \subset A$, соответствующее только хаотическому поведению отображения (1). В ряде работ (см. [2,12–14]) было доказано, что при $j = 1$ и $j = 2$ существуют такие возмущения $\hat{a} = (a_1, a_2, \ldots, a_\tau)$, что при $\hat{a} \in \mathbf{A}_c$ (или $g(a) \in A_c$) возмущенное отображение будет регулярным с устойчивым циклом периода $t = \tau n$. Более того, для одномерных отображений ($j = 1$) справедлив следующий точный результат [5].

Пусть отображение $T_a : x \mapsto f(x, a)$, $x \in M$, $a \in A$, удовлетворяет свойствам: (1) существует подмножество $\sigma \subset M$, такое, что для любых $x_1, x_2 \in \sigma$ найдется значение $a^* \in A$, для которого $f(x_1, a^*) = x_2$; (2) существует критическая точка $x_c \in \sigma$ такая, что $\partial f(x, a)/\partial x|_{x=x_c} \equiv D_x f(x_c, a) = 0$ при любом $a \in A$. Тогда для любых $x_2, x_3, \ldots, x_\tau \in \sigma$ найдутся такие x_1 и a_1, $a_2, \ldots, a_\tau$, что цикл $(x_1, x_2, \ldots, x_\tau)$ будет устойчивым циклом возмущенного отображения $\mathbf{T}_a$ при $\hat{a} = (a_1, \ldots, a_\tau)$.

Для кодирования необходимо уметь оценивать допустимый уровень шума (см. [15]). Это нетрудно сделать, используя следующую оценку [5]. Предположим, что возмущенное отображение $\mathbf{T}_a$

при $\hat{a} = (a_1, a_2, \ldots, a_\tau)$ имеет устойчивый цикл периода τ, $p = (x_1, x_2, \ldots, x_\tau)$. Тогда, если

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

где $i = 1, 2, \ldots, \tau$, $S_a = \max\limits_{x,a} |D_a f(x, a)|$, $L = \max\limits_{x,a} |D_x^2 f(x, a)|$, $S_x = \max\limits_{x,a} |D_x f(x, a)|$, то это отображение имеет также устойчивый цикл $p' = (x_c + \Delta x_1, x_2 + \Delta x_2, \ldots, x_\tau + \Delta x_\tau)$ периода τ при $\hat{a}' = (a_1 + \Delta a_1, a_2 + \Delta a_2, \ldots, a_\tau + \Delta a_\tau)$, причем $|\Delta x_i| \leqslant \delta_x = 1/LS_x^{\tau - 1}$.

На первом этапе кодирования необходимо получить ASCII–коды всех символов, входящих в кодируемый текст. Как известно, в этих кодах каждому символу отвечает единственная тройка чисел. Например, латинской букве „a“ соответствует ASCII–код 97 и числа $n_1 = 0$, $n_2 = 9$, $n_3 = 7$. Далее, каждый член этой тройки интерпретируем как период цикла, существующего в динамической системе. При этом, для того, чтобы избежать присутствия вырожденных циклов (периода 0) и устойчивых точек (циклов периода 1) к каждому n_i, $i = 1, 2, 3$, следует прибавить двойку. Теперь, используя хаотические свойства применяемого отображения (или генератор случайных чисел), составим последовательность, имеющую длину, равную сумме всех n_i, увеличенных на два, плюс 1. Последний элемент используется для начала отсчета периода цикла.

Полученный ряд случайных чисел интерпретируем как последовательность значений динамической переменной x. Для того чтобы она содержала информацию о шифруемых символах, заменим в этой последовательности часть элементов на значения критических точек x_c, т. е. точек, где $f'(a, x)|_{x_c} = 0$. Эти точки должны располагаться друг от друга на расстоянии $n_i + 2$ шагов, начиная с первого. Таким образом, составленная последовательность будет образована подпоследовательностями, число которых равно числу членов в последовательности $n_i + 2$, т. е. числу символов кодируемого текста, умноженному на три. При этом периоды циклов должны равняться значениям $n_i + 2$. Теперь вычислим значения $\hat{a} = a_1, \ldots, a_n$ управляющего параметра, т. е. найдем возмущение, стабилизирующее полученную последовательность циклов. Это нетрудно сделать, рассматривая обратную задачу определения параметров из вида отображения. Поскольку для определенных отображений возмущения $\hat{a}$, приводящие к стабилизации цикла

Таблица 1. Принцип кодирования символов в передаваемой текстовой последовательности

$$\left\{\begin{matrix}\text{Y}\\ \text{символ}\end{matrix}\right\} \to \left\{\begin{matrix}n_1,\ n_2,\ n_3\\ \text{ASCII}-\text{коды}\end{matrix}\right\} \to$$

$$\to \left\{\begin{matrix}\text{циклы}\quad \text{периодов}\quad n_i+2\\ \vert\qquad\qquad\vert\\ \{x_0,\ldots,x_{n_1+2},\ldots,x_{(n_1+2)+n_2+2},\ldots,x_{(n_1+2+n_2+2)+n_3+2}\\ \text{множество динамических переменных}\end{matrix}\right\} \to$$

$$\to \left\{\begin{matrix}\{a_1,\ldots,a_{n_1+2},\{b_1,\ldots,b_{n_2+2}\},\{c_1,\ldots,c_{n_3+2}\}\\ \text{множество параметров}\end{matrix}\right\} \to \left\{\begin{matrix}a_1,\ldots,c_{n_3+2}\\ \text{посл-ть чисел}\end{matrix}\right\}$$

заданного периода, образуют некоторую область в параметрическом пространстве, это можно использовать для кодирования повторяющихся символов посредством случайного выбора параметров из этой области.

Основные этапы кодирования описанным методом представлены в табл. 1. Полученная в результате последовательность $a_1, \ldots, c_{n_3+2}$ (т.е. параметры, а не сообщение) посылается на приемник. Здесь все операции (с некоторыми отличиями, связанными с округлениями), выполняются в обратном порядке, поскольку метод симметричен.

Для обоснования предлагаемого метода необходимо провести статистический анализ и анализ криптостойкости [16]. При статистическом анализе использовалась последовательность значений управляющего параметра длиной 9000, являющаяся кодом сообщения, состоящего из тысячи символов „o“ (лат.). Передача этого символа представляет собой наиболее опасный случай работы описываемого метода защиты, так как его код ASCII суть 111, и информация о каждом „o“ будет содержаться в трех следующих друг за другом циклах периода $n_i + 2 = 1 + 2 = 3$. Повторение таких циклов крайне нежелательно. Удовлетворительные результаты решения поставленной задачи в этом случае позволят говорить о еще большей надежности метода при кодировании других групп символов. В ходе анализа получены следующие данные: коэффициент корреляции $r = 0.0077$, уравнение регрессии $y = 4.9322905 + 0.00769911509x$, среднее значение в выборке $\bar{x} = 4.96478169$. Следовательно, рассматриваемый метод защиты

информации обладает высокой надежностью с точки зрения корреляционного анализа и способен защищать информационные сообщения значительных размеров.

Основными количественными мерами стойкости шифра служат трудоемкость метода криптографического анализа и его надежность [17,18]. Мы провели анализ криптостойкости методом тотального опробования, который заключается в последовательном случайном и равновероятном опробовании без повторений N ключей из множества K. Процесс заканчивается при опробовании k ключей, т.е. если $k = j$, $1 < j < N$, j — номер первого ключа, при котором соответствующий расшифрованный текст признается содержательным, или $k = N$, если такое событие не происходит при любом $j \leqslant N$. Для оценки содержательности расшифровываемого текста вводятся следующие гипотезы: $H(0)$ — текст открытый, $H(1)$ — текст случаен. При составлении вероятностной модели эту оценку определяют следующие ошибки: $\alpha = P(H(1)/H(0))$ — вероятность отбраковки содержательного текста, $\beta = P(H(0)/H(1))$ — вероятность принять несодержательный текст за содержательный. Модель вычисления трудоемкости методом криптографического анализа может быть записана как

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

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

где $\mathrm{E}^{\alpha,\beta}(k)$ — математическое ожидание, характеризующее окончание процесса опробования, N — количество опробованных ключей. Результаты расчета в предположении безошибочной работы механизма принятия решений ($\alpha = 0$, $\beta = 0$) сведены в табл. 2. Для расчета надежности использовалось соотношение

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

Очевидно, надежность метода тотального опробования в предположении безошибочной работы механизма принятия решений ($\alpha = 0, \beta = 0$) получается равной 1.

Таблица 2. Результаты расчета трудоемкости метода

Байт/коэфф.	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}	$6 \cdot 10^8$ years
4	2^{99}	2^{98}	10^{16} лет
5	2^{123}	2^{122}	$1.5 \cdot 10^{23}$ years

Примечание: Левая колонка — количество байтов, отводимое для хранения значения управляющего параметра. Правая колонка — трудоемкость, переведенная в единицы времени на основании сведений о производительности современных суперкомпьютеров.

Таким образом, основными достоинствами данного метода являются следующие: (1) для его реализации может быть использован достаточно широкий класс отображений; (2) в процессе трансляции сама информационная последовательность не передается, посылается лишь сигнал, необходимый для дальнейшей обработки информации; (3) динамическая система, которая является ключом к расшифровке, обладает хаотическими свойствами; (4) декодирование происходит без предварительной синхронизации приемника и передатчика; (5) метод устойчив к наличию внешних шумов; (6) теоретически вариантов кодирования бесконечно много. Что касается практической реализации, то на сегодняшний день разработано сетевое приложение, позволяющее пользователям обмениваться текстовыми сообщениями, защищенными представляемым методом.

Список литературы

[1] *Алексеев В.В., Лоскутов А.Ю.* // ДАН СССР. 1987. Т. 293. № 6. С. 1346–1348.
[2] *Лоскутов А.Ю., Шишмарев А.И.* // Успехи матем. наук. 1993. Т. 48. № 1. С. 169–170.
[3] *Ott E., Grebogi C., Yorke J.A.* // Phys. Rev. Lett. 1990. V. 64. N 11. P. 1196–1199.
[4] *Boccaletti S., Grebogi C., Lai Y.-C.* и др. // Phys. Rev. 2000. V. 329. N 3. P. 103–197.
[5] *Loskutov A.* // Comp. Math. Mod. 2001. V. 12. N 4. P. 314–352.
[6] *Cuomo K.M., Oppenheim A.V.* // Phys. Rev. Lett. 1993. V. 71. N 1. P. 65–68.

[7] *Hayes S., Grebogi C., Ott E., Mark A.* // Phys. Rev. Lett. 1994. V. 73. N 13. P. 1781–1784.
[8] *Kocarev L., Parlitz U.* // Phys. Rev. Lett. 1995. V. 74. N 25. P. 5028–5031.
[9] *Carroll T.L., Pecora L.M.* // Chaos. 1999. V. 9. N 2. P. 445–451.
[10] *Kennedy M.P., Kolumbán G.* // Signal Processing. 2000. V. 80. N 7. P. 1307–1320.
[11] *Fraser B., Yu P., Lookman T.* // Phys. Rev. E. 2002. V. 66. N 1. P. 017202–1–4.
[12] *Loskutov A., Shishmarev A.I.* // Chaos. 1994. V. 4. N 2. P. 351–355.
[13] *Дерюгин А.Н., Лоскутов А.Ю., Терешко В.М.* // Теор. и матем. физика. 1995. Т. 104. N 3. С. 507–512.
[14] *Deryugin A.N., Loskutov A., Tereshko V.M.* // Fractals, Solitons, and Chaos. 1996. V. 7. N 10. P. 1–13.
[15] *Dolnik M., Bollt E.M.* // Chaos. 1998. V. 8. N 3. P. 702–710.
[16] *Simmons G.J.* (ed.). Contemporary Cryptology: The Science of Information Integrity. IEEE Press, Piscataway, N.J., 1992. 656 p.
[17] *Теория и практика обеспечения информационной безопасности* / Ред. П.Д. Зегжда. М.: Изд. агентства „Яхтсмен“, 1996. 298 с.
[18] *Криптография* / Под ред. В.П. Шерстюка, Э.А. Применко. М.: СОЛОН-Р, 2002. 512 с.