электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056.55

Алгоритмы нелинейной динамики в современной криптографии

***Сидоров М.В.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Басараб М.А.,д.ф.-м.н., профессор
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
v.a.matveev@bmstu.ru

Введение

Первым упоминанием задачи связанной с хаотическим поведением динамических систем является задача *n*-тел, за решение которой король Швеции Оскар II в 1890 г. назначил награду. Задача *n*-тел относится к проблеме определения орбит *n* небесных тел, решение которой доказывало бы устойчивость Солнечной системы. Вплоть до 1995 г., никто не мог решить задачу полностью. Тем не менее, Анри Пуанкаре в этом же году получил приз за то, что был близок к решению. Он обнаружил, что орбиты трех и более небесных тел, подверженных взаимному тяготению, являются нестабильными и малопредсказуемыми. Таким образом, родилось математическое понятие хаоса [1]. Начало теории хаоса берется из работы *Tien-Wien Li* и *James A. Yorke* «Period Three Implies Chaos», где авторы впервые вводят само понятие «теория хаоса».

В современном мире теория хаоса имеет очень широкий спектр областей, в которых ей нашлось применение, таких как связь, стабилизация и управление в технике, химия, медицина и многие другие. Например, для совершения гравитационных маневров космических аппаратов для экономии топлива решается задача о трех телах, показанная Пуанкаре. Более глубокий обзор приведен в [1]. Также были попытки создания логических вентилей, основанных на свойствах хаоса, для возможности морфинга типов логики в зависимости от текущих потребностей [2].

Генераторы хаоса

Генераторы хаоса разделяются на два класса: непрерывные и дискретные. Понятие непрерывности и дискретности относятся к временной переменной математических моделей хаотических систем.

Есть множество непрерывных генераторов хаоса, модели которых были получены из самых разнообразных областей физики, биологии, электроники и т.д. Исторически выделяется классическая модель хаотического генератора Лоренца. В общем виде модель представляет собой следующую систему уравнений

$$\begin{cases} \dot{} & -x_1) \\ \dot{} & x_2 - x_1 x_3, \\ \dot{} & \beta x_3 \end{cases} \quad (1)$$

В данной системе бифуркационным параметром является ρ. Сложная хаотическая система блуждает между тремя неустойчивыми равновесными точками, движение системы приобретает непериодический характер — в системе наступает хаос (рис. 1).

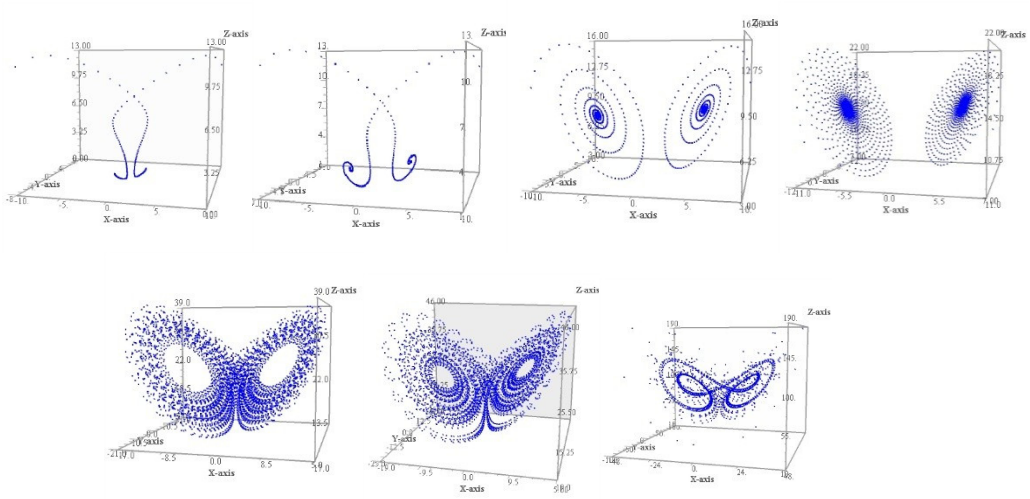

Рис. 1. Эволюция фазового портрета генератора Лоренца: предпоследнее состояние является собственно аттрактором Лоренца; последнее – режим автоколебаний

Так же, из других областей физики и химии выделяются генератор Дуффинга, генератор Рёсслера, использующийся для описания химических реакций, протекающих в реакторе с перемешиванием, генератор Чуа (электронная схема, которую он описывает, стала классическим образцом хаотического автогенератора в радиоэлектронике). Более детальный анализ этих классических схем дан в [3].

Дискретные генераторы хаоса так же еще называют хаотическими отображениями. Данным генераторам соответствует некоторое рекуррентное соотношение. Из самых известных можно выделить:

- логистическое отображение (или отображение Фейгенбаума)

$$x_{n+1} = r_n(1 - x_n). \quad (2)$$

- гауссово отображение, представляющее собой отображение функции Гаусса на прямую $y = x$

$$x_{n+1} = e^{-\alpha x^2} + \beta. \quad (3)$$

Однако при дискретизации временного параметра систем непрерывного состояния, математические модели непрерывных генераторов хаоса так же сводятся к итерационной функции вида

$$x_{n+1} = f\left(x_n, k\right), \quad (4)$$

где k – некоторый управляющий параметр.

В работе [4] наглядно показана разница бифуркационных диаграмм при разном временном параметре для хаотической системы с математической моделью, поведение которой соответствует логистическому отображению (рис. 2).

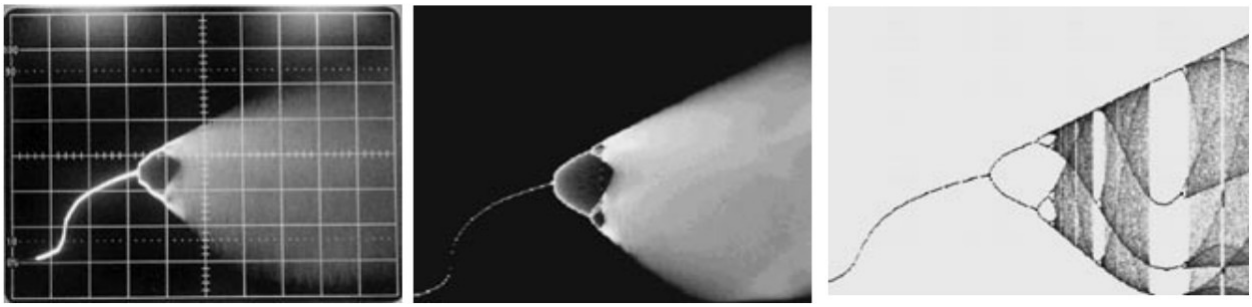

Рис. 2. Бифуркационная диаграмма длинноволнового генератора хаоса [4]: непосредственно слева, физический эксперимент; посередине, численное интегрирование дифференциального уравнения системы, непрерывного времени; справа, адиабатическая аппроксимация, дискретного времени

Для хаотической системы количественной мерой чувствительности, то есть характеристикой экспоненциального разбегания траекторий, находящихся в окрестности некоторой точки, является экспонента Ляпунова:

$$\lambda(x_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \log\left|f'(x_k)\right|, \quad (5)$$

Предел равен среднему значению логарифма производной после n итераций и показывает скорость расхождения траекторий в течение дискретного времени n. Из других количественных мер так же нужно выделить энтропию Колмогорова-Синая, получаемую из экспоненты Ляпунова.

Хаос в криптографии

Согласно Шеннону [5], для защиты от статистического анализа зашифрованных данных, необходимо использовать два метода сокрытия исходных статических распределений: *запутывание (diffusion)* и *распыление (confusion)*. Запутывание обеспечивает сокрытие статических свойств исходного текста для стороннего наблюдателя. Распыление выполняет функции:

1. близкие открытые тексты должны зашифровываться сильно различающиеся шифротексты;
2. близкие ключи должны приводить к сильно различающимся шифротекстам исходного открытого текста.

Необходимо выделить следующие, важные для криптографического приложения, свойства хаотической системы:

- *Чувствительность к начальным условиям*. Небольшие флуктуации начальных состояний параметров системы приводят к значительным изменениям траекторий эволюции параметров. Одним из яркий примеров является «эффект бабочки».
- *Малый горизонт прогноза*. По текущему состоянию невозможно сделать предсказание следующего состояния системы на долгий период.
- *Эргодичность*. Подразумевает, что пространство состояний S хаотической системы не может быть разделено на не нетривиальные непересекающиеся подмножества (относительно соответствующей меры [6]). То есть, если траектория эволюции системы будет начинать с некоторого состояния s_0 из пространства состояний S, мы не сможем определить некоторое подмножество, меньшее чем S, где эта траектория остановится.
- *Смешиваемость (топологическая транзитивность, топологическая смешиваемость)*. Траектория с началом в s_0 после $n \to \infty$ итераций, будет появляться в окрестностях каждой точки с одной и той же вероятностью [7].

То есть, динамическая система тогда будет хаотической, когда все ее траектории ограничены, но быстро расходятся в каждой точке своего фазового пространства.

Чувствительность к начальным условиям соответствует распылению. Смешиваемость и эргодичность должны будут обеспечить запутывание. Малый горизонт прогноза обеспечит устойчивость к реконструкции последовательности по наблюдаемым состояниям системы.

Основная идея хаотической криптографии – использование вышеперечисленных свойств для генерации случайных последовательностей, внешне имеющих абсолютно

случайный вид. В иносказательной форме, для выделения характерной особенности, можно отметить, что хаос является порядком, но более высокого порядка. Для стороннего наблюдателя будет неразличимо стохастическим или хаотическим является поведение системы.

Существует два подхода использования хаотических систем в криптографии [8]. В первом, псевдослучайная последовательность, сгенерированная хаотической системой, используется как ключевой поток для маскирования исходного открытого текста. Методов подобного маскирования на данный момент создано очень много, например [9]. Во втором подходе, открытый текст используется в качестве начального состояния, которое потом посредством хаотичности траекторий эволюции хаотической системы запутываются в результирующее состояние. Первый подход соответствует потоковым шифрам, тогда как второй – блочным. Пример блочного шифрования рассмотрен в работе [10].

В основе потокового шифрования по факту используется генерация псевдослучайных последовательностей символов (битов). Основная идея в данном подходе следующая. Берется некоторая хаотическая система $F : S \to S$, где S – пространство состояний с нормализованной инвариантной мерой μ, определенной на этом пространстве. Цель в том, чтобы разделить пространство на два непересекающихся множества S_0, S_1 таким образом, что $\mu(S_0) = \mu(S_1) = \frac{1}{2}$. Последовательность состояний траектории эволюции системы будет соответствовать некоторой битовой последовательности $\left(b_i(s)\right)_{i=0}^{n}$, где $b_i(s) = 0$, если $s_i \in S_0$ и $b_i(s) = 1$, если $s_i \in S_1$. Подобная конструкции рассматривается в [6].

Возможна и более сложная символьная динамика для пространства большей мощности, в которое будут отображаться состояния динамической системы.

Выводы

В работе был сделан краткий экскурс в теорию хаотических систем, рассмотрены их основные свойства, обеспечивающие их прикладное значение в построение криптографических систем. Такие свойства как чувствительность к начальным условиям, малый горизонт прогноза, эргодичность и смешиваемость (топологическая транзитивность), обеспечивают нам методы, практическая потребность в которых была описана К. Шенноном (запутывание, распыление в смысле ключа, в смысле текста). Рассмотрен один из примеровпостроения генератора псевдослучайных чисел.

Существует множество работ по построению генераторов псевдослучайных последовательностей. В современной криптографии уже существуют криптографические примитивы, основанные на теории хаоса, позволяющие использовать их как для симметричной криптографии, так и для ассиметричной [11].

Список литературы

1. W. Ditto, T. Munakata. Principles and Applications of Chaotic Systems // Communications of the ACM. November 1995, Vol. 38, No. 11, P 96-102
2. Logic from Chaos // MIT Technology Review, June 15, 2006. URL http://www.technologyreview.com/news/405940/logic-from-chaos/ (дата обращения 26.02.13)
3. Шахтарин Б.И. Кобылкина П.И., Сидоркина Ю.А. и др., Генераторы хаотических колебаний. - Москва : Гелиос АВР, 2007.
4. L. Larger, P.-A. Lacourt, S. Poinsot, V. Udaltsov. Chaotic Behaviors of Discrete and Continuous Time Nonlinear Delay Dynamics in Optics //Laser Physics, Vol. 15, No. 9, 2005, P 1209–1216
5. C.E. Shannon. A Mathematical Theory of Communication // Bell System Technical Journal, July 1948, p.623
6. J. Szczepanski, Z. Kotulski. Pseudorandom Number Generators Based on Chaotic Dynamic System. // Open Sys. & Information Dyn. 8, 2001, P 137-146.
7. Птицын Н. Приложение теории детерминированного хаоса в криптографии. –М.: МГТУ им. Н.Э. Баумана, 2002.81 с.
8. J.M. Amigo, L. Kocarev, J. Szczepanski. Theory and practice of chaotic cryptography.
A. Citavicius, A. Jonavicius. An Image encryption using pesudo random bit generator based on a non-linear dynamic chaotic system. WSES TRANSACTIONS on COMMUNICATIONS. September 2009, Issue 9, Volume 8, P 1022-1031.
9. G. Jakimoski, L. Kocarev. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. // IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: FUNDAMENTAL THEORY AND APPLICATIONS, Vol. 48, No. 2, FEBRUARY 2001, P 163-169.
10. Ljupco Kocarev, Shiguo Lian. Chaos-based cryptography. Theory, Algorythms and Applications: Springer-Verlag, Berlin Heldelberg, 2011. 408 c.