4. Marsaglia, G. The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness / G. Marsaglia [Electronic resource]. – Florida State University, 1995.

5. Искусство программирования: в 3 т. Т. 1: Полученные методы / Д.Э. Кнут. – М.: Вильямс, 2007.

6. Харин, Ю.С. Цепь Маркова с частичными связями ЦМ(s, r) и статистические выводы о ее параметрах / Ю.С. арин, А.И. Петлицкий // Дискретная математика. – 2007. – Т. 19, № 2. – С. 109–130.

7. Raftery, A.E. A model for high-order Markov chains / A.E. Raftery // J. Royal Statistical Society. – 1985. – V. B-47, № 3. – P. 528–539.

8. Харин, Ю.С. Алгоритмы статистического анализа цепей Маркова с условной глубиной памяти / Ю.С. Харин, М.В. Мальцев // Информатика. – 2011. – №1. – С. 34–43.

9. Харин, Ю.С. Статистическая проверка гипотез о параметрах цепи Маркова условного порядка / Ю.С. Харин, М.В. Мальцев // Весці НАН Беларуси, Серыя. фіз.-мат. навук. – 2012. – №3. – С. 5–12.

10. Meier, W. The self-shrinking generator / W. Meier, O Staffelbach // Advances in Cryptology – EUROCRYPT 94. 1995. Springer-Verlag LNSC 950. – P. 205–214.

11. Основы криптографии / А.П. Алферов [и др.]. М.: Гелиос АРВ, 2001.

Abstract

The paper deals with Markov chain of conditional order, which is a parsimonious model of discrete time series. The model was used for statistical analysis of cryptographic generators output sequences.

The results of computer experiments are presented.

Поступила в редакцию 18.05.2013 г.

ПОВТОРЯЕМОСТЬ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СОСТОЯНИЙ ПОЛНОЦИКЛОВЫХ АВТОНОМНЫХ АВТОМАТОВ

УДК 519.711.2,519.713.2.

А.Н. Гайдук,
НИИ ППМИ БГУ, г. Минск

Аннотация

В настоящей работе рассматривается полноцикловой генератор псевдослучайной последовательности. Попадание генератора псевдослучайной последовательности в ранее использованное состояние означает повторную выработку выходной последовательности, что является крайне нежелательным явлением. Анализ этого события для случая когда длины вырабатываемой псевдослучайной последовательности полноциклового генератора являются случайными величинами приведен в работе [1], случай когда длины вырабатываемой псевдослучайной последовательности являются произвольными фиксированными величинами рассмотрен в работе [2]. В настоящей работе для случая отрезков равной длины вырабатываемой псевдослучайной последовательности получена более простая модель, которая согласуется с результатами работы [1]-[2].

Введение

Будем рассматривать в качестве генератора псевдослучайной последовательности автономный автомат $U = (S, Z, \varphi, \psi)$, где $S = \{s_1, s_2, ..., s_N\}$ – конечное множество состояний, $Z = \{0,1\}$ – конечное множество выходных символов, $\varphi : S \to S$ – функция переходов, $\psi : S \to Z$ – функция выходов. Канонические уравнения функционирования автономного автомата U имеют вид:

$$s(t+1) = \varphi(s(t))$$
$$z(t) = \psi(s(t)), \quad t \geq 0,$$

$s(0)$ – начальное состояние.

Под состоянием генератора понимаем состояние описывающего его автономного автомата.

Постановка задачи

Пусть в процессе вычислений используется n отрезков последовательности псевдослучайных чисел, полученных с помощью полноциклового генератора. Будем отождествлять начальное состояние $s_i = (s_{i,1}, ..., s_{i,m})$ i-го отрезка последовательности псевдослучайных чисел с числом $X_i = \sum_{k=1}^{m} s_{i,k} 2^{m-k}$. Через L_i обозначим длину i-го отрезка.

Будем считать, что случайные величины $X_1, ..., X_n$ независимы в совокупности и при всех i:

$$P(X_i = k) = \frac{1}{2^m}, \; k = 0, ..., 2^m - 1.$$

Требуется оценить вероятность перекрытия n отрезков длин $L_i = \overline{1,n}$.

Повторяемость последовательностей состояний случайной длины (модель М1)

В работе [1] исследовался случай, когда длины отрезков $L_1, ..., L_n$ являются случайными величинами:

$$P(l_i = k) = p_k, \; k = 1, ..., N,$$

причем

$$P(1 \leq L_i \leq \frac{N}{2}) = 1.$$

В [1] доказана теорема, которая позволяет построить оценки снизу и сверху для вероятности неперекрытия отрезков $L_1, ..., L_n$.

Повторяемость последовательностей состояний произвольной длины (модель М2)

В работе [2] получены результаты для отрезков произвольных длины. Пусть отрезки имеют следующие длины: $L_1, ..., L_n$, где, вообще говоря, $L_i \neq L_j$ при $i \neq j$. Перекрытие отсутствует, если все пары отрезков не имеют перекрытий.

Теорема 1. Вероятность не перекрытия n отрезков длин $L_1, ..., L_n$, $\sum_{j=1}^{n} L_j = L$, при цикле длины N автомата равна

$$\frac{(n-1)! C_{N-L+n-1}^{n-1}}{N^{n-1}}. \qquad (1)$$

Повторяемость последовательностей состояний равной длины (модель М3)

Для случая отрезков равной длины в настоящей работе предлагается более простая формула. Предположим, что длины отрезков удовлетворяют следующему соотношению: $L_1 = L_2 = ... = L_n = L_0$. Перекрытие отсутствует, если все пары отрезков не имеют перекрытий.

Теорема 2. Если мы можем пренебречь величиной $\frac{nL_0}{N}$, тогда вероятность не перекрытия n отрезков длин $L_1 = L_2 = ... = L_n = L_0$, при цикле длины N автомата равна

$$\frac{(M-1)...(M-n+1)}{M^{n-1}}, \quad M = \frac{N}{2L_0}. \qquad (2)$$

Доказательство

Действительно, поскольку мы пренебрегаем величиной $\frac{nL_0}{N}$, то мы можем свести задачу к следующей. Т.к. у нас отрезки равной длины, то мы их заменим точками, а общее число состояний автомата уменьшим в $2L_0$ раз. Обозначим $M = \frac{N}{2L_0}$. Тогда количество способов, которыми мы можем выбрать произвольную точку, равно M. А для того, чтобы не происходило перекрытий, мы будем выбирать следующую точку так, чтобы она не совпадала ни с какой предыдущей. Тогда искомая вероятность равна (2).

Заключение

Нами было рассмотрено 3 модели:

– повторяемость последовательностей состояний равной длины;

– повторяемость последовательностей состояний произвольной длины;

– повторяемость последовательностей состояний случайной длины.

Приведем некоторые численные результаты. Пусть $N = 10^{10}$, а длины отрезков неслучайны и одинаковы: $L_1 = L_2 = ... = 10^4$. В таблице 1 представлены вероятности, вычисленные по моделям М2 и М3, а также вытекающих из теоремы 2 работы [1] оценок снизу и сверху для вероятностей не перекрытия отрезков модели М1.

Таблица 1 – Связь между моделями М1, М2 и М3

n	Модель М3	Модель М2	Модель М1	
			Оценка снизу	Оценка сверху
200	0.961	0.961	0.961	0.961
400	0.852	0.852	0.852	0.853
600	0.698	0.698	0.697	0.700
800	0.527	0.527	0.525	0.531
1000	0.368	0.368	0.365	0.372
1200	0.236	0.237	0.234	0.242
1400	0.140	0.140	0.138	0.145
1600	0.077	0.077	0.074	0.081
1800	0.039	0.039	0.037	0.042
2000	0.018	0.018	0.017	0.020

Литература:

1. Михайлов, В.Г. О повторяемости датчика псевдослучайных чисел при его многократном использовании / В.Г. Михайлов // Теория вероятн. и ее примен. – 1995. – Т. 40. – в. 4. – С. 786–797.

2. Бабаш, А.В. Криптография / А.В. Бабаш, Г.П. Шанкин. – М.: Солон-Р. – 2002. – 512 с.

Abstract

The full-cyclic generator of pseudorandom sequence is considered. Hit of the generator in earlier used state means that output sequence will be used twice that is the extremely undesirable phenomenon. The analysis of this event for a case when lengths of output sequences of the full-cyclic generator are random variables is provided in [1], a case when lengths of output sequences are any fixed values is considered in [2]. In this article for a case of equal length output sequences simpler model that is consistent with the results of [1]-[2] is presented.

Поступила в редакцию 18.05.2013 г.

ОЦЕНКА ЗАЩИЩЕННОСТИ ЦИФРОВЫХ СИГНАЛОВ АМ, ЧМ, ФМ, КАМ В КАНАЛАХ УТЕЧКИ ИНФОРМАЦИИ

УДК 621.397.7:004.056.57

Д.С. Рябенко, В.К. Железняк
ПГУ, г. Полоцк

Аннотация

Исследуется оптимальный сигнал для оценки защищенности цифровых каналов утечки информации. Технология технической защиты информации формирует обобщенные требования к теории и технике передачи систем сигналов. Рассматривается система сигналов, используемая для передачи информации как совокупность сигналов, объединяемых единым правилом построения. Известно, что помехоустойчивость – одно из основных требований к системе передачи. Предложены оптимальная система сигналов, обеспечивающая максимальную помехоустойчивость при минимальных отношениях энергии бита к спектральной плотности мощности шума в каналах утечки информации, методы оценки защищенности дискретных систем сигналов в каналах утечки информации при воздействии шумов высокого уровня типа белого гауссовского шума, а также выбор и обоснование оптимального