



Кафедра радиотехнических и телекоммуникационных систем

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
Технологический институт
Федерального государственного образовательного учреждения
высшего профессионального образования
«Южный федеральный университет»
ПРИОРИТЕТНЫЙ НАЦИОНАЛЬНЫЙ ПРОЕКТ
«ОБРАЗОВАНИЕ»**

**Руководство
к лабораторной работе**

**Исследование генераторов
псевдослучайных последовательностей**

Для студентов специальностей 210402, 210405

РТФ

Таганрог 2007

Составители: В.А. Алехин, В.В. Шеболков

Руководство к лабораторной работе “Исследование генераторов псевдослучайных последовательностей”. – Таганрог: Изд-во ТРТУ, 2007. – 20с.

Руководство составлено для студентов специальностей 210402, 210304, 210405. Позволяет в рамках лабораторного практикума изучить свойства псевдослучайных последовательностей, применяемых для потоковых шифров в системах передачи дискретных сообщений, и принципы построения генераторов таких последовательностей.

Табл. 3. Илл. 4. Библиогр.: 3 назв.

Рецензент В.Г. Сердюков, канд. техн. наук, доцент кафедры РТС ТРТУ.

1. Теоретические сведения

1.1. Вводные замечания

Генераторы последовательностей псевдослучайных чисел применяются в технике для решения широкого круга задач, связанных с кодированием и шифрованием информации. Требования, предъявляемые к таким генераторам, могут изменяться в зависимости от решаемой задачи, однако можно выделить ряд наиболее распространенных из таких требований. Прежде всего, это существование алгоритма, который позволял бы многократно воспроизводить любую из псевдослучайных последовательностей при заданных начальных условиях и внешних воздействиях. Следующими по важности являются требования относительно статистических свойств формируемых последовательностей, т.е. распределения генерируемых чисел и их корреляционных связей. Немаловажным требованием к генераторам последовательностей псевдослучайных чисел является удобство и простота технической реализации соответствующих алгоритмов.

В задачах защиты информации и криптографии к генераторам псевдослучайных последовательностей (ПСП) предъявляют следующие основные требования: 1) распределение генерируемых чисел должно быть близким к равномерному; 2) период корреляции наибольший при заданной сложности генератора; 3) корреляционная функция ПСП не должна иметь побочных максимумов; 4) в ПСП не должно встречаться длинных серий одинаковых символов.

Таким образом, при реализации генераторов ПСП необходимо решать две взаимосвязанные задачи:

- а) выбор алгоритма формирования ПСП;
- б) проверка статистических свойств сформированных последовательностей.

Ниже рассматриваются три алгоритма формирования ПСП: полиномиальный (конгруэнтные генераторы), линейный рекуррентный (линейные рекуррентные последовательности – ЛРП, М-последовательности – последовательности максимальной длины) и один из алгоритмов формирования составных ЛРП. Два последних алгоритма нашли применение в задачах защиты информации в системах сотовой связи третьего поколения (в частности алгоритм А5 стандарта GSM).

1.2. Конгруэнтные генераторы

Конгруэнтные (полиномиальные) генераторы – это генераторы, алгоритм работы которых может быть представлен в виде полинома :

$$X_n = (a_k X_{n-1}^k + a_{k-1} X_{n-1}^{k-1} + \dots + a_2 X_{n-1}^2 + a_1 X_{n-1} + a_0) \bmod m,$$

где X_n , ($n=0,1,\dots$) – числа генерируемой ПСП;

a_i ($i=0,\dots,k$) – коэффициенты полинома;

m – модуль (некоторая константа, которая задает максимальное значение ПСП).

Рассматриваемый алгоритм реализует рекуррентную процедуру вычисления элементов ПСП, перед началом которой необходимо задать нулевой элемент последовательности X_0 .

Линейными конгруэнтными генераторами называют генераторы, реализующие алгоритм

$$X_n = (aX_{n-1} + b) \bmod m.$$

Таблица 1

Константы для линейных конгруэнтных генераторов

Переполнение при	a	b	m
2^{20}	106	1283	6075
2^{21}	211	1663	7875
2^{22}	421	1663	7875
2^{23}	430 936 1366	2531 1399 1283	11979 6655 6075
2^{24}	171 859 419 967	11213 2531 6173 3041	53125 11979 29282 14406
2^{25}	141 625 1541 1741 1291 205	28411 6571 2957 2731 4621 29573	134456 31104 14000 12960 21870 139968
2^{26}	421 1255 281	17117 6173 28411	81000 29282 134456
2^{27}	1093 421 1021 1021	18257 54773 24631 25673	86436 259200 116640 121500
2^{28}	1277 741 2041	24749 66037 25673	117128 312500 121500

Окончание табл. 1

Переполнение при	a	b	m
2^{29}	2311	25367	120050
	1807	45289	214326
	1597	51749	244944
	1861	49297	233280
	2661	36979	175000
	4081	25673	121500
	3661	30809	145800
2^{30}	3877	29573	139968
	3613	45289	214326
	1366	150889	714025
2^{31}	8121	28411	134456
	4561	51349	243000
	7141	54773	259200
2^{32}	9301	49297	233280
	4096	150889	714025

Переменные a , b и m – константы: a – множитель, b – инкремент, и m – модуль. Ключом служит задаваемое значение X_0 .

Период такого генератора не превышает m . Если a , b и m выбраны правильно (например, b должно быть взаимно простым с m числом), то генератор будет создавать последовательность с максимальным периодом (максимальной длиной), и этот период будет равен m . Некоторые наборы констант для получения максимального периода можно найти в приведенной табл.1. Все они обеспечивают генерацию ПСП с максимальным периодом и удовлетворяют спектральному тесту на случайность.

Преимуществом линейных конгруэнтных генераторов является их простота и высокая скорость работы за счет малого количества операций

Линейные конгруэнтные генераторы не рекомендуют использовать в криптографии, так как их алгоритмы легко вскрываются. Известны также алгоритмы вскрытия генераторов с производящими полиномами второй $X_n = (aX_{n-1}^2 + bX_{n-1} + c) \bmod m$ и третьей $X_n = (aX_{n-1}^3 + bX_{n-1}^2 + cX_{n-1} + d) \bmod m$ степени.

Разработаны способы вскрытия любого полиномиального генератора [1], что показывает ограниченные возможности применения конгруэнтных генераторов в криптографировании. Еще одним слабым местом таких генераторов является возможность переполнения разрядной сетки процессора при некорректном выборе величины m .

Однако линейные конгруэнтные генераторы сохраняют свою полезность в ряде других задач, например для моделирования. Они просты и при использовании в эмпирических тестах демонстрируют

хорошие статистические характеристики. Полезную информацию о линейных конгруэнтных генераторах и более глубокие теоретические сведения можно найти в работах [1, 2].

1.3. Линейные рекуррентные последовательности

Линейные рекуррентные последовательности формируются в соответствии с алгоритмом

$$X_k = a_{n-1}X_{k-1} + a_{n-2}X_{k-2} + \dots + a_2X_{k-n+2} + a_1X_{k-n+1} + a_0X_{k-n},$$

в котором умножение и суммирование осуществляются по модулю некоторого числа m .

В приведенной формуле $a_{n-1}, a_{n-2}, \dots, a_1, a_0$ – некоторое множество постоянных коэффициентов, набор которых существенно влияет на формируемую ЛРП.

Нетрудно заметить отличие ЛРП от рассмотренных выше конгруэнтных ПСП: если в последних при формировании очередного элемента ПСП участвует только предыдущий элемент, то при формировании очередного элемента ЛРП используется гораздо большее количество предшествующих элементов. Этим реализуется один из важных принципов повышения криптоустойчивости шифров: распространение влияния одного элемента шифра на другие элементы.

В задачах защиты информации широкое распространение получили ЛРП в поле двоичных чисел. Генераторы таких ЛРП (рис.1) реализуются на основе линейных регистров сдвига (ЛРС) с обратной связью. Их теория прекрасно проработана, потоковые шифры на базе сдвиговых регистров использовались в криптографии задолго до появления электроники.

Такой генератор состоит из двух частей: ЛРС, блока весовых коэффициентов a_0, \dots, a_n и сумматора, реализующих функции обратной связи. ЛРС представляет собой последовательность триггерных ячеек D_i , в каждой из которых хранится 1 бит информации. Этот бит за один такт работы регистра может перемещаться в соседнюю триггерную ячейку влево или вправо – в зависимости от схемы регистра. Если регистр содержит n триггерных ячеек, то регистр называется n -битовым сдвиговым регистром. Всякий раз, когда нужно извлечь очередной бит информации, все биты сдвигового регистра сдвигаются на 1 позицию вправо. Значение нового крайнего левого бита является функцией всех остальных битов регистра. В качестве выходной величины рассматриваемого генератора обычно выбирают значение бита в одной из ячеек регистра (обычно крайней правой).

Нетрудно заметить, что размер множества возможных значений ЛРП не превышает величины $M=2^n-1$ – количества возможных со-

стояний регистра сдвига, поэтому все значения генерируемой ПСП периодически повторяются. (Число внутренних состояний и период равны M , потому что заполнение ЛРС нулями приведет к тому, что сдвиговый регистр будет выдавать бесконечную последовательность нулей.)

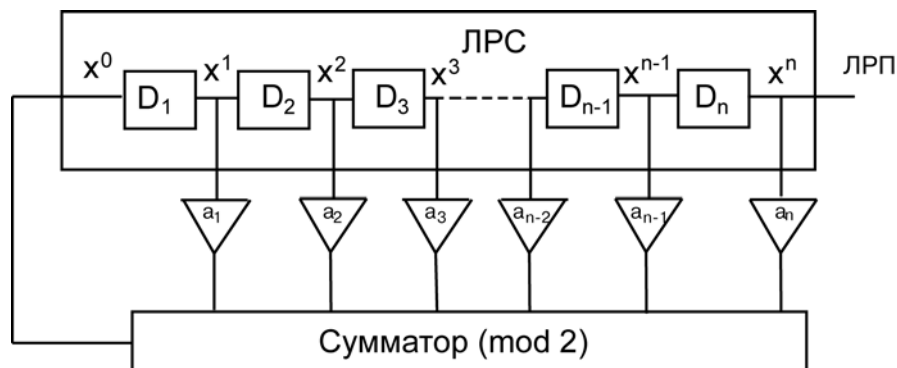


Рис. 1. Генератор ЛРП на основе регистра сдвига

Простейшим генератором ЛРП является ЛРС с функцией обратной связи в виде сумматора по модулю 2 некоторых битов регистра. Перечень этих битов (он соответствует набору коэффициентов a_0, \dots, a_n) называют отводной последовательностью (tap sequence). Простота функции обратной связи позволила выполнить хороший теоретический анализ таких генераторов. Только при определенных наборах отводных последовательностей ЛРС циклически пройдет через все M внутренних состояний, такие ПСП имеют максимальный период и называются M -последовательностями.

Для того, чтобы конкретный ЛРС имел максимальный период, многочлен, образованный из отводной последовательности

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + 1,$$

должен быть примитивным в поле двоичных чисел. Степень многочлена равна длине сдвигового регистра. Примитивный многочлен степени n – это неприводимый многочлен, на который делится многочлен $x^M + 1$, (где $M = 2^n - 1$) и который не является делителем $x^d + 1$ для всех чисел d , являющихся делителями $2^n - 1$.

Способ нахождения примитивных многочленов данной степени по модулю 2 в общем случае неизвестен. Задачу решают случайным выбором многочленов и проверкой, не являются ли они примитивными. Программы для решения этой задачи содержат многие математические пакеты программ.

Некоторые примитивные многочлены по модулю 2 приведены в табл.2 [2]. Например, запись (32, 7, 5, 3, 2, 1, 0) означает, что многочлен $p(x) = x^{32} + x^7 + x^5 + x^3 + x^2 + x^1 + x^0 = x^{32} + x^7 + x^5 + x^3 + x^2 + x^1 + 1$ примитивен в поле двоичных чисел.

Таблица 2

Некоторые примитивные многочлены в поле двоичных чисел

1<n<50	50<n<100	101<n<150	151<n<200	n>200
(1, 0)	(50, 4, 3, 2, 0)	(100, 37, 0)	(150, 53, 0)	(201, 14, 0)
(2, 1, 0)	(51, 6, 3, 1, 0)	(100, 8, 7, 2, 0)	(151, 3, 0)	(201, 17, 0)
(3, 1, 0)	(52, 3, 0)	(101, 7, 6, 1, 0)	(151, 9, 0)	(201, 59, 0)
(4, 1, 0)	(53, 6, 2, 1, 0)	(102, 6, 5, 3, 0)	(151, 15, 0)	(201, 79, 0)
(5, 2, 0)	(54, 8, 6, 3, 0)	(103, 9, 9)	(151, 31, 0)	(202, 55, 0)
(6, 1, 0)	(54, 6, 5, 4, 3, 2, 0)	(104, 11, 10, 1, 0)	(151, 39, 0)	(207, 43, 0)
(7, 1, 0)	(55, 24, 0)	(105, 16, 0)	(151, 43, 0)	(212, 105, 0)
(7, 3, 0)	(55, 6, 2, 1, 0)	(106, 15, 0)	(151, 46, 0)	(218, 11, 0)
(8, 4, 3, 2, 0)	(56, 7, 4, 2, 0)	(107, 9, 7, 4, 0)	(151, 51, 0)	(218, 15, 0)
(9, 4, 0)	(57, 7, 0)	(108, 31, 0)	(151, 63, 0)	(218, 71, 0)
(10, 3, 0)	(57, 5, 3, 2, 0)	(109, 5, 4, 2, 0)	(151, 66, 0)	(218, 83, 0)
(11, 2, 0)	(58, 19, 0)	(110, 6, 4, 1, 0)	(151, 67, 0)	(225, 32, 0)
(12, 6, 4, 1, 0)	(58, 6, 5, 1, 0)	(111, 10, 0)	(151, 70, 0)	(225, 74, 0)
(13, 4, 3, 1, 0)	(59, 7, 4, 2, 0)	(111, 49, 0)	(152, 6, 3, 2, 0)	(225, 88, 0)
(14, 5, 3, 1, 0)	(59, 6, 5, 4, 3, 1, 0)	(113, 9, 0)	(153, 1, 0)	(225, 97, 0)
(15, 1, 0)	(60, 1, 0)	(113, 15, 0)	(153, 8, 0)	(225, 109, 0)
(16, 5, 3, 2, 0)	(61, 5, 2, 1, 0)	(113, 30, 0)	(154, 9, 5, 1, 0)	(231, 26, 0)
(17, 3, 0)	(62, 6, 5, 3, 0)	(114, 11, 2, 1, 0)	(155, 7, 5, 4, 0)	(231, 34, 0)
(17, 5, 0)	(63, 1, 0)	(115, 8, 7, 5, 0)	(156, 9, 5, 3, 0)	(234, 31, 0)
(17, 6, 0)	(64, 4, 3, 1, 0)	(116, 6, 5, 2, 0)	(157, 6, 5, 2, 0)	(234, 103, 0)
(18, 7, 0)	(65, 18, 0)	(117, 5, 2, 1, 0)	(158, 8, 6, 5, 0)	(236, 5, 0)
(18, 5, 2, 1, 0)	(65, 4, 3, 1, 0)	(118, 33, 0)	(159, 31, 0)	(250, 103, 0)
(19, 5, 2, 1, 0)	(66, 9, 8, 6, 0)	(119, 8, 0)	(159, 34, 0)	(255, 52, 0)
(20, 3, 0)	(66, 8, 6, 5, 3, 2, 0)	(119, 45, 0)	(159, 40, 0)	(255, 56, 0)
(21, 2, 0)	(67, 5, 2, 1, 0)	(120, 9, 6, 2, 0)	(160, 5, 3, 2, 0)	(255, 82, 0)
(22, 1, 0)	(68, 9, 0)	(121, 18, 0)	(161, 18, 0)	(258, 83, 0)
(23, 5, 0)	(68, 7, 5, 1, 0)	(122, 6, 2, 1, 0)	(161, 39, 0)	(266, 47, 0)
(24, 4, 3, 1, 0)	(69, 6, 5, 2, 0)	(123, 2, 0)	(161, 60, 0)	(270, 133, 0)
(25, 3, 0)	(70, 5, 3, 1, 0)	(124, 37, 0)	(162, 8, 7, 4, 0)	(282, 35, 0)
(26, 6, 2, 1, 0)	(71, 6, 0)	(125, 7, 6, 5, 0)	(163, 7, 6, 3, 0)	(282, 43, 0)
(27, 5, 2, 1, 0)	(71, 5, 3, 1, 0)	(126, 7, 4, 2, 0)	(164, 12, 6, 5, 0)	(286, 69, 0)
(28, 3, 0)	(72, 10, 9, 3, 0)	(127, 1, 0)	(165, 9, 8, 3, 0)	(286, 73, 0)
(29, 2, 0)	(72, 6, 4, 3, 2, 1, 0)	(127, 7, 0)	(166, 10, 3, 2, 0)	(294, 61, 0)
(30, 6, 4, 1, 0)	(73, 25, 0)	(127, 63, 0)	(167, 6, 0)	(322, 67, 0)
(31, 3, 0)	(73, 4, 3, 2, 0)	(128, 7, 2, 1, 0)	(170, 23, 0)	(333, 2, 0)
(31, 6, 0)	(74, 7, 4, 3, 0)	(129, 5, 0)	(172, 2, 0)	(350, 53, 0)
(31, 7, 0)	(75, 6, 3, 1, 0)	(130, 3, 0)	(174, 13, 0)	(366, 29, 0)
(31, 13, 0)	(76, 5, 4, 2, 0)	(131, 8, 3, 2, 0)	(175, 6, 0)	(378, 43, 0)
(32, 7, 6, 2, 0)	(77, 6, 5, 2, 0)	(132, 29, 0)	(175, 16, 0)	(378, 107, 0)
(32, 7, 5, 3, 2, 1, 0)	(78, 7, 2, 1, 0)	(133, 9, 8, 2, 0)	(175, 18, 0)	(390, 89, 0)
(33, 13, 0)	(79, 9, 0)	(134, 57, 0)	(175, 57, 0)	(462, 73, 0)
(33, 16, 4, 1, 0)	(79, 4, 3, 2, 0)	(135, 11, 0)	(177, 8, 0)	(521, 32, 0)
(34, 8, 4, 3, 0)	(80, 9, 4, 2, 0)	(135, 16, 0)	(177, 22, 0)	(521, 48, 0)
(34, 7, 6, 5, 2, 1, 0)	(80, 7, 5, 3, 2, 1, 0)	(135, 22, 0)	(177, 88, 0)	(521, 158, 0)
(35, 2, 0)	(81, 4, 0)	(136, 8, 3, 2, 0)	(178, 87, 0)	(521, 168, 0)
(36, 6, 5, 4, 2, 1, 0)	(82, 9, 6, 4, 0)	(137, 21, 0)	(183, 56, 0)	(607, 105, 0)
	(82, 8, 7, 6, 1, 0)	(138, 8, 7, 1, 0)	(194, 87, 0)	(607, 147, 0)
	(83, 7, 4, 2, 0)	(139, 8, 5, 3, 0)	(198, 65, 0)	(607, 273, 0)

$1 < n < 50$	$50 < n < 100$	$101 < n < 150$	$151 < n < 200$	$n > 200$
(36, 11, 0)	(84, 13, 0)	(140, 29, 0)		(1279, 216, 0)
(37, 6, 4, 1, 0)	(84, 8, 7, 5, 3, 1, 0)	(141, 13, 6, 1, 0)		(1279, 418, 0)
(37, 5, 4, 3, 2, 1, 0)	(85, 8, 2, 1, 0)	(142, 21, 0)		(2281, 715, 0)
	(86, 6, 5, 2, 0)	(143, 5, 3, 2, 0)		(2281, 915, 0)
(38, 6, 5, 1, 0)	(87, 13, 0)	(144, 7, 4, 2, 0)		(2281, 1029, 0)
(39, 4, 0)	(87, 7, 5, 1, 0)	(145, 52, 0)		(3217, 67, 0)
(40, 5, 4, 3, 0)	(88, 11, 9, 8, 0)	(145, 69, 0)		(3217, 576, 0)
(41, 3, 0)	(88, 8, 5, 4, 3, 1, 0)	(146, 5, 3, 2, 0)		(4423, 271, 0)
(42, 7, 4, 3, 0)	(89, 38, 0)	(147, 11, 4, 2, 0)		(9689, 84, 0)
(42, 5, 4, 3, 2, 1, 0)	(89, 51, 0)	(148, 27, 0)		
	(89, 6, 5, 3, 0)	(149, 10, 9, 7, 0)		
(43, 6, 4, 3, 0)	(90, 5, 3, 2, 0)			
(44, 6, 5, 2, 0)	(91, 8, 5, 1, 0)			
(45, 4, 3, 1, 0)	(91, 7, 6, 5, 3, 2, 0)			
(46, 8, 7, 6, 0)	(92, 6, 5, 2, 0)			
(46, 8, 5, 3, 2, 1, 0)	(93, 2, 0)			
	(94, 21, 0)			
(47, 5, 0)	(94, 6, 5, 1, 0)			
(48, 9, 7, 4, 0)	(95, 11, 0)			
(48, 7, 5, 4, 2, 1, 0)	(95, 6, 5, 4, 2, 1, 0)			
	(96, 10, 9, 6, 0)			
(49, 9, 0)	(96, 7, 6, 4, 3, 2, 0)			
(49, 6, 5, 4, 0)	(97, 6, 0)			
	(98, 11, 0)			
	(98, 7, 4, 3, 1, 0)			
	(99, 7, 5, 4, 0)			

Все примитивные полиномы содержат нечетное число коэффициентов. Если полином $p(x)$ примитивен, то примитивен и многочлен $x^n p(x^{-1})$, поэтому каждый элемент таблицы на самом деле определяет два примитивных многочлена.

Например, если многочлен $(a, b, 0)$ примитивен, то примитивен и многочлен $(a, a-b, 0)$. Если примитивен многочлен $(a, b, c, d, 0)$, то примитивен и $(a, a-d, a-c, a-b, 0)$. В развернутой записи это означает следующее: если примитивен $x^a + x^b + 1$, то примитивен и $x^a + x^{a-b} + 1$, если примитивен $x^a + x^b + x^c + x^d + 1$, то примитивен и $x^a + x^{a-d} + x^{a-c} + x^{a-b} + 1$. Наиболее просто реализуются примитивные трехчлены, так как для генерации нового бита нужно просуммировать по mod 2 только два бита сдвигового регистра. Однако такие разреженные многочлены являются источником потенциальной слабости для вскрытия алгоритма. Для криптографических алгоритмов гораздо лучше использовать примитивные многочлены, у которых отлично от нуля большое количество коэффициентов. Применяя такие многочлены, например, в качестве части ключа, можно использовать значительно более короткие ЛРС.

Сами по себе ЛРС являются хорошими генераторами псевдослучайных последовательностей, но они обладают некоторыми нежела-

тельными неслучайными свойствами. Последовательные биты связаны между собой линейной зависимостью, что делает их бесполезными для шифрования. Для ЛРС длиной n внутреннее состояние определяется предыдущими n выходными битами генератора. Даже если схема обратных связей неизвестна злоумышленнику, она может быть определена по фрагменту последовательности длиной не менее $2n$.

Кроме того, большие случайные числа, генерируемые с использованием идущих подряд битов этой последовательности, сильно коррелированы и для некоторых типов приложений являются вовсе не случайными. Несмотря на это ЛРС часто используются для создания алгоритмов шифрования.

Линейная сложность. Анализировать потоковые шифры часто проще, чем блочные. Например, важным параметром, используемым для анализа генераторов на базе ЛРС, является линейная сложность (linear complexity), или длина линейного интервала. Она определяется как длина n самого короткого ЛРС, который может имитировать исследуемый генератор. Любая последовательность, генерированная конечным автоматом над конечным полем, имеет конечную линейную сложность. Линейная сложность важна, потому что известны алгоритмы, с помощью которых можно определить структуру обратных связей этого ЛРС, проанализировав $2n$ битов потока ПСП.

В любом случае высокая линейная сложность генератора не обязательно гарантирует криптостойкость ПСП, но низкая линейная сложность является предпосылкой к недостаточной криптостойкости.

Корреляционная независимость. Высокую линейную сложность пытаются получить, линейно или нелинейно объединяя результаты некоторых выходных последовательностей. При этом опасность состоит в том, что одна или несколько внутренних выходных последовательностей — часто просто выходы отдельных ЛРС — могут быть связаны общим ключевым потоком и вскрыты методами линейной алгебры. Часто такое вскрытие называют корреляционным вскрытием.

Основной идеей корреляционного вскрытия является обнаружение некоторой корреляции между элементами последовательности, отстоящими друг от друга на некоторый интервал. Тогда, наблюдая выходную последовательность, можно получить информацию о длине ЛРС и отводной последовательности.

1.4. Генераторы составных ЛРП на базе ЛРС

Линейный генератор составных ЛРП. Основная идея построения генератора ПСП на базе ЛРС заключается в следующем: определенным образом объединяются несколько ПСП, полученных от ЛРС с различными длинами и различными многочленами обратной связи. Ключ шифрования определяет начальные состояния ЛРС. Бит выхода представляет собой функцию некоторых битов регистров ЛРС. Эта функция называется комбинирующей функцией, а генератор в целом – комбинационным генератором (рис.2).

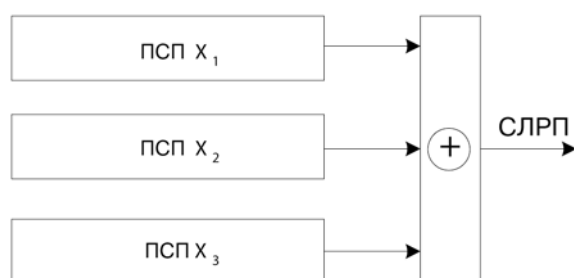


Рис. 2. Комбинационный генератор

Для вскрытия алгоритмов работы этих генераторов используют корреляцию символов составной ЛРП. Чтобы затруднить злоумышленнику нахождение содержания регистра и вскрытие алгоритма формирования ПСП, необходимо усложнять способ комбинирования исходных ПСП в составную последовательность. Поэтому не стоит применять генераторы ПСП на базе ЛРС, описанные в литературе. Большей частью они представляют лишь теоретический интерес.

Генератор Геффа. В этом генераторе ПСП используются три генератора ПСП, объединенные с помощью мультиплексора (рис.3). Сигналы от двух генераторов ПСП подаются на информационные входы мультиплексора, а третий генерирует для него управляющую последовательность.

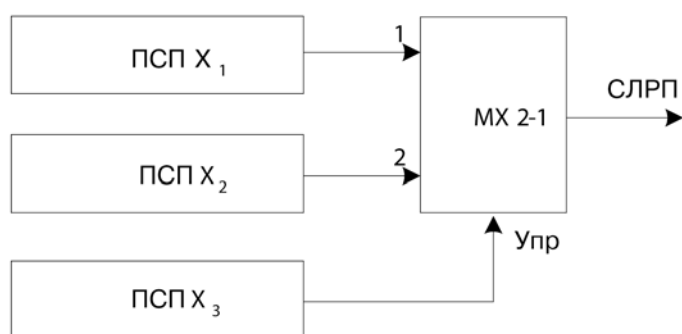


Рис. 3. Генератор Геффа

Если x_1 , x_2 и x_3 – ПСП на выходах трех ЛРС, то ПСП на выходе генератора Геффа можно описать следующим образом:

$$b = (x_2 \& x_3) \vee (x_1 \& \bar{x}_3).$$

Период генерируемой последовательности равен наименьшему общему кратному периодов последовательностей трех генераторов. Если степени трех примитивных многочленов обратной связи взаимно просты, период генерируемой последовательности будет равен произведению периодов трех ЛРС.

Генератор Геффа не устойчив против корреляционного вскрытия [1]. Например, если примитивные многочлены состоят только из трех членов и длина самого большого ЛРС равна n , то для восстановления внутренних состояний всех трех ЛРС нужен фрагмент выходной последовательности длиной $3n$ бит.

2. Методы испытаний генераторов ПСП

При испытаниях генераторов случайных и псевдослучайных последовательностей необходимо провести статистические тесты для выяснения распределения вероятностей генерируемых случайных величин и их статистической независимости.

Оценка вида распределения

Для оценки вида распределения случайной величины (СВ) можно использовать один из известных из математической статистики критериев согласия экспериментальных и теоретических результатов.

Этот подход базируется на теории проверки статистической гипотезы H_1 о том, что выборка x_1, x_2, \dots, x_n некоторой СВ X принадлежит рассматриваемому распределению $w(x)$ против альтернативы H_0 : рассматриваемая выборка не принадлежит $w(x)$. В статистических критериях используется некоторая мера отклонения U экспериментального распределения $\hat{w}(x)$ от теоретического $w(x)$, и сравнивают ее с некоторым порогом u_0 . По результатам этого сравнения принимается решение в пользу одной из гипотез H_1 или H_0 .

В качестве экспериментального распределения $\hat{w}(x)$ обычно используют гистограмму $h(x)$, построенную по выборке x_1, x_2, \dots, x_n . Для построения $h(x)$ интервал определения (x_0, x_m) случайной величины X разбивают на m интервалов: $(x_0, x_1), (x_1, x_2), \dots, (x_{m-1}, x_m)$, оп-

ределяют количество случайных величин k_i , $i = (1, \dots, m)$, попавшее в каждый из указанных интервалов, и находят оценки вероятностей p_i^* попадания случайной величины X в каждый из указанных интервалов:

$$p_i^* = \frac{k_i}{n}.$$

Результаты расчетов сводят в таблицу (табл.3), которую и называют гистограммой. Графическое изображение гистограммы позволяет получить наглядное представление о виде распределения случайной величины X (рис.4).

Таблица 3

Гистограмма выборки x_1, x_2, \dots, x_n

(x_0, x_1)	(x_1, x_2)	(x_2, x_3)	...	(x_{m-1}, x_m)
p_1^*	p_2^*	p_3^*	...	p_m^*

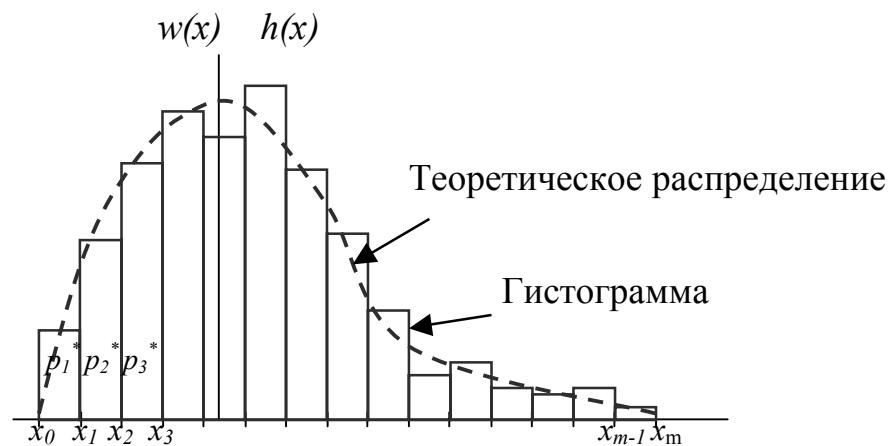


Рис. 4. Теоретическое распределение $w(x)$ случайной величины X и гистограмма $h(x)$ выборки x_1, x_2, \dots, x_n

В качестве меры отклонения гистограммы $h(x)$ от $w(x)$ естественно выбрать среднеквадратическое отклонение $U = \sum_{i=1}^m c_i (p_i^* - p_i)^2$, где

$p_i = \int_{x_{i-1}}^{x_i} w(x) dx$ — вероятность попадания случайной величины X в интервал (x_{i-1}, x_i) ; c_i — некоторый весовой множитель. Если положить $c_i = \frac{n}{p_i}$, то при больших n случайная величина U обладает весьма интересным свойством: ее распределение практически не зависит от $w(x)$, а зависит только от m , и при увеличении n оно приближается к хорошо известному в теории вероятностей χ^2 — распределению.

При таком выборе c_i мера отклонения обычно обозначается следующим образом:

$$U = \chi^2 = n \sum_{i=1}^m \frac{(p_i^* - p_i)^2}{p_i} = \sum_{i=1}^m \frac{(k_i - np_i)^2}{np_i}. \quad (1)$$

Распределение χ^2 характеризуется плотностью вероятности

$$w_\alpha(u) = \begin{cases} \frac{1}{2^{\frac{\alpha}{2}} \Gamma(\frac{\alpha}{2})} u^{\frac{\alpha}{2}-1} \exp(-\frac{u}{2}), & u \in (0, \infty), \\ 0 & u \in (-\infty, 0], \end{cases}$$

где $\Gamma(\frac{\alpha}{2}) = \int_0^\infty t^{\frac{\alpha}{2}-1} \exp(-t) dt$ – гамма-функция.

Распределение χ^2 зависит от параметра α , который называют числом степеней свободы.

$$\alpha = m - s,$$

где s – число наложенных на экспериментальное распределение ограничений. Примерами таких ограничений могут быть следующие соотношения:

$\sum_{i=1}^m p_i^* = 1$ – условие нормировки (это ограничение действует всегда);

$\sum \tilde{x}_i p_i = M[X]$ – равенство математических ожиданий экспериментального и теоретического распределений;

$\sum_{i=1}^m (\tilde{x}_i - M[X])^2 p_i^* = D[X]$ – равенство дисперсий.

Распределение χ^2 табулировано (табл. П.1 [3]). По таблицам и рассчитанным значениям U и α можно найти вероятность того, что случайная величина с распределением χ^2 превысит U . Если эта вероятность невелика (на практике $p < 0,1$), то гипотеза H_1 отбрасывается как неправдоподобная.

Таким образом, схема применения критерия χ^2 включает три этапа:

1) строится гистограмма выборки x_1, x_2, \dots, x_n и по формуле (1) определяется значение $U = \chi^2$;

2) определяется число степеней свободы $\alpha = m - s$, где s – число наложенных ограничений;

3) по U и α определяется вероятность того, что случайная величина с распределением χ^2 превзойдет U ; если эта вероятность мала, то гипотеза H_1 отвергается как неправдоподобная.

Оценка статистической независимости

Для оценки статистической независимости случайных величин в первом приближении можно использовать коэффициент корреляции r , характеризующий линейные связи между СВ. В общем случае коэффициент корреляции между СВ выборками (x_1, x_2, \dots, x_n) и (y_1, y_2, \dots, y_l) определяется формулой

$$r = \frac{1}{\sqrt{D[X]D[Y]}} \sum_{i=1}^n \sum_{j=1}^l (x_i - M[X])(y_j - M[Y])p_{ij},$$

где $M[X], M[Y], D[X], D[Y]$ – математические ожидания и дисперсии СВ X и Y ;

p_{ij} – вероятность совместного появления x_i и y_j .

Следует заметить, что коэффициент корреляции характеризует не любые, а только линейные связи между X и Y . Таким образом, равенство нулю коэффициента корреляции будет означать, что между X и Y не будет только линейной статистической зависимости, из чего не следует их статистическая независимость.

При анализе ПСП одним из наиболее важных критериев является выявление их периодичности, т.е. статистической связи между СВ, генерируемыми в разные моменты времени.

В этом случае процесс на выходе генератора ПСП рассматривают как эргодический и коэффициент корреляции определяют по формуле

$$r(j) = \frac{1}{D[x]} \sum_{i=1}^K (x_i - M[x])(x_{i-j} - M[x]).$$

Здесь x_{i-j} – сдвинутая на j тактов относительно x_i ПСП генератора; K – число элементов (тактов) анализируемой последовательности.

Если в этой формуле полагать $x_{i-j} = 0$ при $i - j < 0$, то говорят о непериодическом коэффициенте корреляции. Наряду с этим рассматривают периодический коэффициент корреляции, когда при $i - j < 0$ полагают $x_{i-j} = x_{K+(i-j)}$, т.е. вычисляют $i - j$ по модулю K .

Изменяя j от 0 до K выявляют значения j , при которых коэффициент корреляции $r(j)$ близок к 1. Это значение j указывает на период ПСП.

3. Домашняя подготовка

1. Изучить алгоритмы работы генераторов ПСП.
2. Выбрать из табл. 1 примитивный полином 4 – 5 порядка, изобразить функциональную схему генератора ЛРП и построить формируемую им ПСП.

3. Построить ПСП, формируемую генератором Геффа, для произвольных полиномов 3 – 4 порядка.
4. Изучить методы анализа ПСП.
5. Для одной из построенных ПСП построить гистограмму и проверить по критерию χ^2 гипотезу о соответствии полученной ПСП равномерному распределению.
6. По периодическому коэффициенту корреляции оценить период одной из построенных ПСП.

4. Лабораторное задание

1. Лабораторное исследование выполняется с помощью программы PSP_Gen, которая позволяет моделировать работу генераторов ПСП и исследовать их наиболее важные характеристики.
2. Загрузить программу PSP_Gen в память ЭВМ, изучить ее интерфейс и правила проведения исследований.
3. Исследовать с помощью программы PSP_Gen работу генераторов ПСП, использованных при домашней подготовке. Сопоставить полученные результаты с результатами домашних расчетов.
4. Выполнить исследование линейных конгруэнтных генераторов, заданных типовыми наборами исходных данных. Сделать выводы о влиянии выбора коэффициентов алгоритма на корреляционные свойства ПСП и вид ее распределения. Подобрать 2 – 3 набора коэффициентов, при которых выполнялись бы требования к ключевым последовательностям в криптографии.
5. Выполнить исследование генераторов ПСП на основе ЛРС, полиномы которых использовались при домашней подготовке. Сопоставить результаты исследования с результатами домашней подготовки. Исследовать характеристики рассматриваемых генераторов, если для функции обратной связи применяется примитивный полином и когда это условие не выполняется. Сопоставить длину полинома с периодом ПСП. Сделать выводы о влиянии выбора коэффициентов полинома на корреляционные свойства ПСП и вид ее распределения. Подобрать 2–3 набора коэффициентов полинома, при которых выполнялись бы требования к ключевым последовательностям в криптографии.
6. Выполнить исследование составных ЛРП на основе сумматора по модулю 2 и мультиплексора. Сопоставить результаты исследования с результатами домашней подготовки. Исследовать характеристики рассматриваемых генераторов для случаев, когда длины образующих полиномов одинаковы, кратны и являются взаимно простыми числами. Сопоставить периоды полученных ПСП. Сделать

выводы о влиянии выбора коэффициентов полинома на корреляционные свойства ПСП и вид ее распределения. Подобрать 2–3 набора коэффициентов полинома, при которых выполнялись бы требования к ключевым последовательностям в криптографии.

7. Оформить отчет по работе и сделать выводы по работе.

5. Содержание отчета по работе

Отчет по работе должен содержать:

а) результаты выполнения домашнего задания (функциональные схемы генераторов ПСП, рассчитанные для выбранных полиномов ПСП, гистограммы и коэффициенты корреляции для них);

б) результаты выполнения лабораторного задания: сопоставление теоретических и экспериментальных результатов, полиномы генераторов ПСП, полученные при подборе ПСП с нужными статистическими свойствами, гистограммы и коэффициенты корреляции для них;

в) анализ результатов работы и выводы по ней.

Контрольные вопросы

1. Каким требованиям должны удовлетворять ПСП, используемые в задачах защиты информации?

2. Назовите критерии статистической независимости выборки случайных величин.

3. Приведите пример расчета периодического и непериодического коэффициентов корреляции.

4. Для чего используется гистограмма выборки случайных величин? Как она строится?

5. Каким образом проверяются гипотезы о принадлежности выборки случайных величин некоторому распределению?

6. Каким образом используется критерий χ^2 для проверки гипотезы о виде распределения ПСП? Приведите пример применения этого критерия.

7. Конгруэнтные генераторы, их свойства, требования к коэффициентам таких генераторов.

8. Возможна ли аппаратная реализация конгруэнтных генераторов? Если нет, – обоснуйте это, если да, – приведите пример построения функциональной схемы такого генератора.

9. Линейные регистры сдвига, алгоритм их работы, функциональная схема, управляющие сигналы, область применения.

10. Приведите примеры построения функциональной и принципиальной схем регистров сдвига, проиллюстрируйте их работу временными диаграммами.

11. Генераторы ЛРП на основе регистров сдвига. Требования к функции обратной связи.

12. М-последовательности и их свойства. Структура генератора М-последовательности.

13. Приведите пример построения генератора ПСП на основе регистра сдвига с обратными связями. Проиллюстрируйте его работу временными диаграммами.

14. Составные ЛРП и их свойства. Приведите пример построения составной ЛРП.

15. Приведите примеры построения составных ЛРП на основе объединения нескольких более коротких ЛРП. Проиллюстрируйте примеры временными диаграммами.

16. Сформируйте М-последовательность на основе полинома 4-го порядка и сложите ее поразрядно по модулю 2 с копией этой последовательности, циклически сдвинутой на 1, 2, 3 разряда. Сравните полученные последовательности между собой и сформулируйте вывод.

17. Сформируйте М-последовательность на основе полинома 4-го порядка и сложите поразрядно по модулю 2 три или четыре ее копии циклически сдвинутые на 1, 2, 3 разряда. Сделайте вывод и на основе этого постройте генератор, позволяющий получать последовательности с любым возможным сдвигом относительно последовательности, снимаемой с последнего разряда ЛРС.

18. Предложите и сформулируйте алгоритм исключения тупикового (нулевого) состояния ЛРС, формирующего М-последовательность и изобразите схему такого генератора.

Библиографический список

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2005. – 229с.
2. У. Питерсон Коды, исправляющие ошибки. – М.: Сов. радио, 1978
3. Е.С. Вентцель Теория вероятностей. – М.: Наука, 1974.

Таблица П.1

Значения χ^2 в зависимости от параметров p и α

α	p													
	0,99	0,98	0,95	0,90	0,80	0,70	0,50	0,30	0,20	0,10	0,05	0,02	0,01	0,001
1	0,000	0,001	0,004	0,016	0,064	0,148	0,455	1,074	1,642	2,71	3,84	5,41	6,64	10,83
2	0,020	0,040	0,103	0,211	0,446	0,713	1,386	2,41	3,22	4,60	5,99	7,82	9,21	13,82
3	0,115	0,185	0,352	0,584	1,005	1,424	2,37	3,66	4,64	6,25	7,82	9,84	11,34	16,27
4	0,297	0,429	0,711	1,064	1,649	2,20	3,36	4,88	5,99	7,78	9,49	11,67	13,28	18,46
5	0,554	0,752	1,145	1,610	2,34	3,00	4,35	6,06	7,29	9,24	11,07	13,39	15,09	20,5
6	0,872	1,134	1,635	2,20	3,07	3,83	5,35	7,23	8,56	10,64	12,59	15,03	16,81	22,5
7	1,239	1,564	2,17	2,83	3,82	4,67	6,35	8,38	9,80	12,02	14,07	16,62	18,48	24,3
8	1,646	2,03	2,73	3,49	4,59	5,53	7,34	9,52	11,03	13,36	15,51	18,17	20,1	26,1
9	2,09	2,53	3,32	4,17	5,38	6,39	8,34	10,66	12,24	14,68	16,92	19,68	21,7	27,9
10	2,56	3,06	3,94	4,86	6,18	7,27	9,34	11,78	13,44	15,99	18,31	21,2	23,2	29,6
11	3,05	3,61	4,58	5,58	6,99	8,15	10,34	12,90	14,63	17,28	19,68	22,6	24,7	31,3
12	3,57	4,18	5,23	6,30	7,81	9,03	11,34	14,01	15,81	18,55	21,0	24,1	26,2	32,9
13	4,11	4,76	5,89	7,04	8,63	9,93	12,34	15,12	16,98	19,81	22,4	25,5	27,7	34,6
14	4,66	5,37	6,57	7,79	9,47	10,82	13,34	16,22	18,15	21,1	23,7	26,9	29,1	36,1
15	5,23	5,98	7,26	8,55	10,31	11,72	14,34	17,32	19,31	22,3	25,0	28,3	30,6	37,7
16	5,81	6,61	7,96	9,31	11,15	12,62	15,34	18,42	20,5	23,5	26,3	29,6	32,0	39,3
17	6,41	7,26	8,67	10,08	12,00	13,53	16,34	19,51	21,6	24,8	27,6	31,0	33,4	40,8
18	7,02	7,91	9,39	10,86	12,86	14,44	17,34	20,6	22,8	26,0	28,9	32,3	34,8	42,3
19	7,63	8,57	10,11	11,65	13,72	15,35	18,34	21,7	23,9	27,2	30,1	33,7	36,2	43,8
20	8,26	9,24	10,85	12,44	14,58	16,27	19,34	22,8	25,0	28,4	31,4	35,0	37,6	45,3
21	8,90	9,92	11,59	13,24	15,44	17,18	20,3	23,9	26,2	29,6	32,7	36,3	38,9	46,8
22	9,54	10,60	12,34	14,04	16,31	18,10	21,3	24,9	27,3	30,8	33,9	37,7	40,3	48,3
23	10,20	11,29	13,09	14,85	17,19	19,02	22,3	26,0	28,4	32,0	35,2	39,0	41,6	49,7
24	10,86	11,99	13,85	15,66	18,06	19,94	23,3	27,1	29,6	33,2	36,4	40,3	43,0	51,2
25	11,52	12,70	14,61	16,47	18,94	20,9	24,3	28,2	30,7	34,4	37,7	41,7	44,3	52,6
26	12,20	13,41	15,38	17,29	19,82	21,8	25,3	29,2	31,8	35,6	38,9	42,9	45,6	54,1
27	12,88	14,12	16,15	18,11	20,7	22,7	26,3	30,3	32,9	36,7	40,1	44,1	47,0	55,5
28	13,56	14,85	16,93	18,94	21,6	23,6	27,3	31,4	34,0	37,9	41,3	45,4	48,3	56,9
29	14,26	15,57	17,71	19,77	22,5	24,6	28,3	32,5	35,1	39,1	42,6	46,7	49,6	58,3
30	14,95	16,31	18,49	20,6	23,4	25,5	29,3	33,5	36,2	40,3	43,8	48,0	50,9	59,7

**Алехин Владимир Алексеевич
Шеболков Виктор Васильевич**

**Руководство к лабораторной работе
Исследование генераторов
псевдослучайных последовательностей**

Для студентов специальностей 210402,210405

Ответственный за выпуск Алёхин В.А.
Редактор Маныч Э.И.
Корректор Селезнева Н.И.

ЛР №020565 от 23.06. 1997г. Подписано к печати _____ г.

Бумага офсетная. Печать офсетная.

Формат 60x84_{1/16}

Усл.п.л. – 1,2. Уч.-изд.л. – 1,0

Заказ №_____ Тираж экз.

«С»

Издательство Технологического института
Южного федерального университета
ГСП 17А, Таганрог, 28, Некрасовский, 44
Типография Технологического института
Южного федерального университета
ГСП 17А, Таганрог, 28, Энгельса, 1