

АНАЛИЗ СВОЙСТВ РЕГИСТРОВ СДВИГА С НЕЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ ВТОРОГО ПОРЯДКА ГЕНЕРИРУЮЩИХ, ПОСЛЕДОВАТЕЛЬНОСТЬ С МАКСИМАЛЬНЫМ ПЕРИОДОМ

А.В. ПОТИЙ, Н.А. ПОЛУЯНЕНКО

В данной работе рассмотрена модель генератора псевдослучайной последовательности на основе регистров сдвига с нелинейной обратной связью второго порядка. Сформулированы требования по вычислению полиномов, генерирующих выходные последовательности с максимально возможным периодом, дана оценка количества таких полиномов.

A pseudorandom sequence generator model based on shift registers with nonlinear second order feedback is considered. Requirements to calculating polynomials that provide generation of output sequences with a maximum possible period are formulated and estimation of the number of such polynomials is given.

ВВЕДЕНИЕ

Сегодня одним из важных криптографических примитивов являются поточные шифры. Как правило, данные шифры состоят из одного или нескольких регистров сдвига с обратной связью. Широкое использование регистров сдвига с обратной связью получили благодаря их простой аппаратной реализации. Существуют различные пути введения нелинейности в выходные последовательности данных регистров [1]. Одним из таких подходов является введение нелинейной функции в обратную связь регистров. К недостатку такого подхода следует отнести то, что на сегодняшний день даже такую простую характеристику, как период формируемой регистром сдвига с нелинейной обратной связью (РСНОС) гаммы, трудно определить. Существуют и другие подходы [2, 3, 4], например, использование нелинейной функции для комбинирования нескольких последовательностей. Период выходной последовательности может быть найден из периодов используемых последовательностей. Третьим подходом является использование нелинейных функций для комбинирования выходов определенных ячеек регистра сдвига с линейной обратной связью. Четвертым подходом является использование управляющих сдвиговых регистров, в котором одни регистры управляют движением других регистров.

Как показано в литературе [5], важную роль, в настоящее время, играют системы генерации случайных чисел основанные на регистрах сдвига с нелинейной обратной связью (РСНОС). Преимуществами таких систем, по сравнению с регистрами сдвига с линейной обратной связью, являются:

- более высокая стойкость (в частности линейная сложность);
- более сложный, по сравнению с РСЛОС, криптоанализ, отсутствие хорошо разработанного математического аппарата;
- большее количество комбинаций обратных связей, что позволяет реализовать схемы, основанные на одной базовой модели (фиксированном количестве ячеек регистров сдвига) и различных долговременных ключах, или же когда требуется

выполнить большое количество шифраторов (например, при серийном производстве), но необходимо обеспечить несовместимость различных партий.

В данной работе авторы рассматривают общую модель регистра сдвига с нелинейной обратной связью, а также формулируют требования, при которых значительно увеличивается вероятность нахождения полинома генерирующего выходную последовательность с максимальным периодом.

1. ОБЩАЯ МОДЕЛЬ РСНОС ВТОРОГО ПОРЯДКА

Рассмотрим систему генерации псевдослучайной двоичной последовательности (ПСП) основанной на РСНОС. В качестве обратной связи будем использовать побитовое сложение (обозначенное знаком $\oplus$) и нелинейную функцию – умножения (обозначенное знаком $\otimes$). Обозначим через L количество регистров сдвига используемых в системе. На рис. 1 показана такая модель РСНОС при $L = 3$.

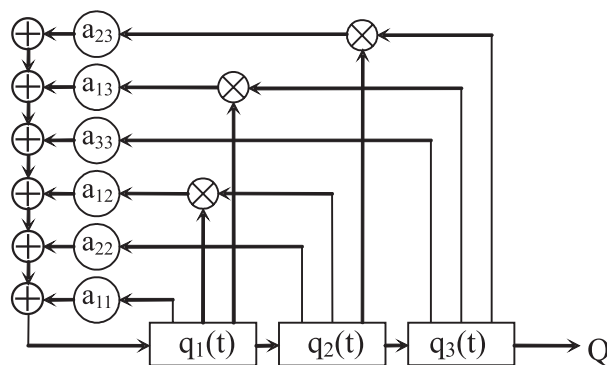


Рис. 1. Общий вид генератора ПСП основанного на РСНОС при $L = 3$, где $a_{ij} \in \{0,1\}$ – блок умножения, $q_i(t) \in \{0,1\}$ – значение i -го регистра в момент времени t , $\oplus$ – знак суммы, $\otimes$ – знак умножения, Q – генерируемая последовательность бит

Здесь блок умножения определяет наличие обратной связи. Так, при $a_{ij} = 1$ умножение a_{ij} равносильно наличию связи, а при $a_{ij} = 0$ умножение на a_{ij} равносильно отсутствию связи. В общем случае,

при такой системе, обратную связь можно задать следующим полиномом:

$$q_i(t+1) = \sum_{i=1}^L \sum_{j=i}^L a_{ij} q_i(t) q_j(t), \quad (1)$$

здесь мы учитываем, что $q_i \cdot q_i = q_i$, т.е. умножение значения регистра самого на себя не дает никакого изменения и поэтому на рис. 1 знак $\otimes$ между i и i регистром опущен.

В нашей нелинейной функции обратной связи присутствуют слагаемые из произведения между двумя регистрами, назовем такую нелинейность — *нелинейностью второго порядка*. Если будут присутствовать произведения между тремя и более регистрами, то будем такую сложность называть третьего и более высокого порядка. Однако изучение нелинейности выше второго порядка выходит за рамки данной статьи и поэтому рассмотрена не будет.

Заметим, что если все коэффициенты в блоке умножения $a_{ij} = 0$ для всех $i \neq j$, то такой частный случай рассматриваемой модели будет представлять собой РСЛОС.

Обозначим через n_L полное количество коэффициентов в блоке умножения, т.е. максимально возможное количество $a_{ij} \neq 0$. Для РСНОС второго порядка n_L определяется однозначно для каждого L по формуле:

$$n_L = \frac{L \cdot (L+1)}{2}, \quad (2)$$

где L — количество регистров сдвига.

Заметим, что при РСЛОС количество обратных связей, которыми можно варьировать, равно L (т.е. $n_L = L$).

Поскольку любой РСНОС является машиной конечных состояний, то как отмечено в [6] генерируемая им ПСП неизбежно будет периодична с периодом T . Основным параметром для оценки сложности предсказания последующих разрядов последовательности является линейная сложность (L_r) ПСП. Характерным показателем T является максимально возможный период ($T_{\max}$) для заданного числа L . Так как нулевое состояние всех регистров является запрещенным, максимально возможное число состояний устройства, а значит и $T_{\max}$ определяется как:

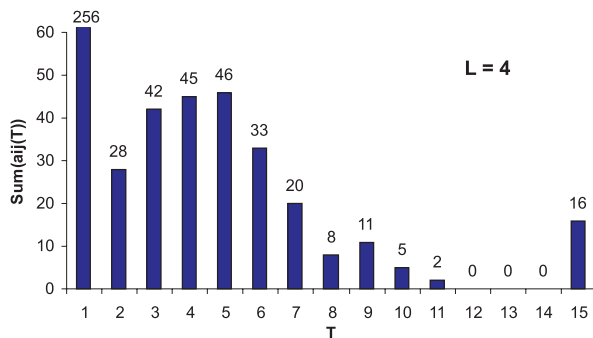
$$T_{\max} = 2^L - 1. \quad (3)$$

Для вычисления L_r используем алгоритм Берлекампа-Мессии, суть которого подробно изложена в [7] и по этой причине здесь не приводится.

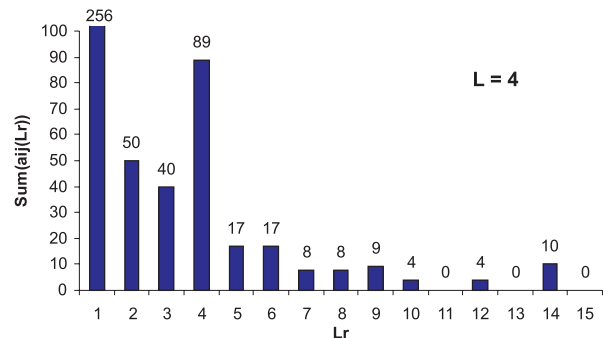
Требования к виду РСНОС второго порядка для формирования последовательности с максимальным периодом.

Сформулируем требования, которым должна отвечать комбинация коэффициентов a_{ij} (т.е. вид обратной связи), при условии выполнении которых генерируется двоичная последовательность с периодом $T = T_{\max}$ и обеспечивается максимальное значение сложности L_r .

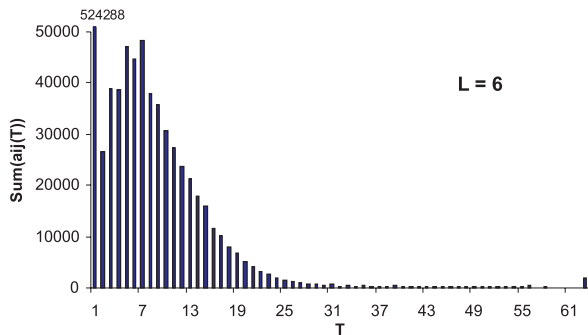
Требование 1. Для обеспечения максимального периода линейный коэффициент обратной связи от последнего регистра должен всегда присутствовать, т.е.:



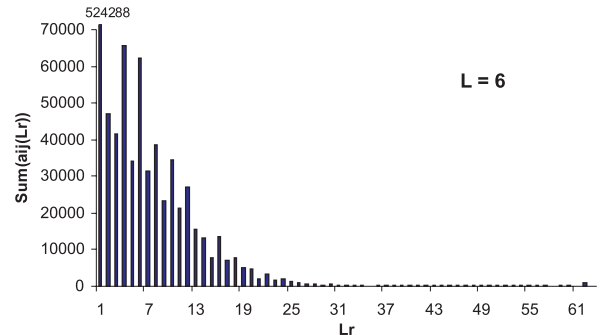
а



б



в



г

Рис. 2. Количество сгенерированных последовательностей РСНОС в зависимости от их периода (а, в) и линейной сложности (б, г) для $L = 4$ и 6 соответственно, при полном переборе a_{ij} (кроме коэффициента a_{LL} , он оставался = 1)

$$a_{LL} = 1.$$

Действительно, если период последовательности равен $T_{\max}$, следовательно, должно быть состояние регистров, при котором $q_1(t)=0, q_2(t)=0, \dots, q_{L-1}(t)=0, q_L(t)=1$, в этом случае $q_1(t+1)=1$ возможно лишь при $a_{LL}=1$.

С учетом первого требования был проведен расчет периода T и линейной сложности L_r для $L=4$ и $L=6$ путем полного перебора всех возможных значений a_{ij} . На рис. 2 показаны результаты расчетов. По оси ординат приведено распределение количества комбинаций $a_{ij}=1$, соответствующее допустимым значениям T и L_r .

Следует обратить внимание, что ровно половина из разрешенных (с учетом требования 1) комбинаций дает $T=1$. При изучении комбинаций a_{ij} , которые дают $T=1$, замечаем, что в этом случае сумма всех $a_{ij}=1$ является нечетным числом. Рассмотрим состояния регистров при их начальном заполнении равном 1, при этом любое произведение регистров даст 1, а сумма любого нечетного количества единиц (по модулю 2) также будет равна 1. Учитывая, что любое первоначальное заполнение (для РСНОС с максимальным периодом) должно пройти состояние, когда все регистры равны 1, получаем заикливание с $T=1$. Беря во внимание вышеизложенное, сформулируем следующее требование, которому должен отвечать РСНОС второго порядка для обеспечения $T=T_{\max}$.

Требование 2. Сумма всех ненулевых коэффициентов обратной связи a_{ij} должна быть четным числом, т.е.:

$$\sum_{ij} a_{ij} - \text{четное число.}$$

Остановимся более подробно на сумме коэффициентов a_{ij} . Выполним расчет всех РСНОС второго порядка для $L=6$ и, с учетом требований 1 и 2, для $L=7$. Просуммируем все коэффициенты $a_{ij} \neq 0$ только из того множества комбинаций a_{ij} , которые дают $T=T_{\max}$. Результаты расчетов приведены на рис. 3.

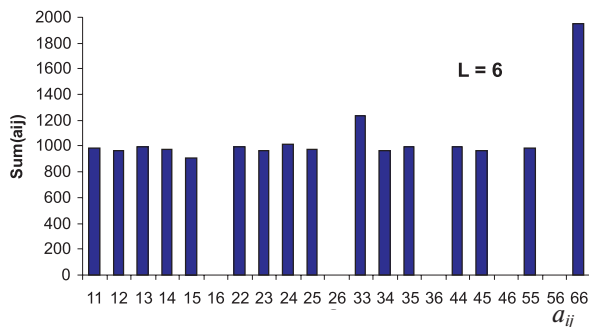
Из приведенных гистограмм (рис. 3 а, б) распределения ненулевых коэффициентов a_{ij} видно, что существуют коэффициенты, которые не принимают участие в генерации максимального периода. Все остальные коэффициенты (кроме $a_{LL}=1$ из требования 1) встречаются примерно равное количество раз. Изучив полученные результаты для РСНОС второго порядка с $L=4,5,6,7$, можно сформулировать еще одно требование, которому должны удовлетворять коэффициенты обратной связи, генерирующие последовательность с максимальным периодом.

Требование 3. Не должно быть нелинейной обратной связи, полученной от выходного регистра и любого другого, т.е.:

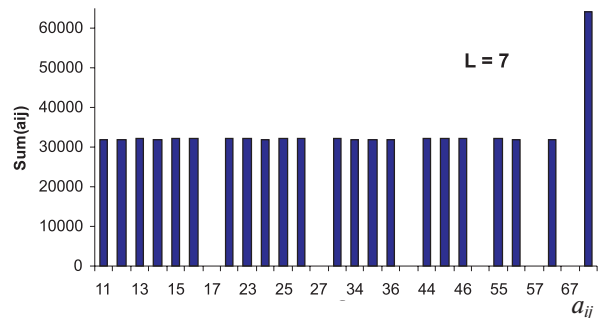
$$\forall a_{iL} = 0, i = \overline{1, L-1}.$$

Рассмотрим, что происходит в РСНОС второго порядка, не удовлетворяющего 3 требованию, и покажем, что требование 3 справедливо для любого значения L .

Для определенности будем рассматривать только те случаи, когда в полиноме всегда присутствует $a_{LL}=1$. Из требования 1 мы можем отки-



а



б

$i \backslash j$	1	2	3	4	5	6
1	984	1000	1236	1000	984	1952
2	968	968	968	968	0	
3	996	1016	996	0		
4	972	972	0			
5	908	0				
6	0					

в

$i \backslash j$	1	2	3	4	5	6	7
1	31996	32116	32266	32266	32116	31996	64056
2	31768	32122	31924	32122	31768	0	
3	32068	31890	31890	32068	0		
4	31942	32048	31942	0			
5	32070	32070	0				
6	32160	0					
7	0						

г

Рис. 3. Гистограмма распределения суммы коэффициентов обратной связи для полного множества значений a_{ij} , которые порождают последовательность с максимальным периодом для РСНОС второго порядка с $L=6$ (а) и $L=7$ (б) и их числовые значения (в, г — соответственно)

нуть все остальные, так как они нам однозначно не дадут примитивного полинома.

Рассмотрим, что происходит при генерации последовательности РСНОС второго порядка, которые не отвечают этому требованию, а также докажем справедливость 3 требования для любой длины регистра.

Наличие коэффициента $a_{iL} = 1 (i \in \{1, L-1\})$ приводит к появлению не колец (т.е. ряда состояний, которые проходят РСНОС, переходя из одного состояния в другое, число таких состояний конечно и равно T (см. рис. 4 а), а петель (т.е. разные исходные состояния регистра приводят к одному и тому же результирующему состоянию). Продемонстрируем изложенное на примере.

Рассмотрим РСНОС второго порядка длины $L=3$, который задается различными полиномами (см. рис. 4). Случай a – полином является примитивным; b – полином не является примитивным, но соответствует 3 требованию (не удовлетворяет 2 требованию); v и z – полиномы соответствуют 3 требованию.

Рассмотрим последовательности всевозможных полиномов длины $L=3$, у которых хотя бы один коэффициент $a_{iL} = 1$. Обнаруживаем следующую закономерность:

1) если $a_{13}=1$, то пара состояний регистра (1,1,1) и (1,1,0), а также (1,0,1) и (1,0,0) даст всег-

да одно и тоже состояние регистра, а пара (0,1,1) и (0,1,0) разное независимо от других $a_{ij}=1 (j \neq L)$;

2) если $a_{23}=1$, то пара состояний регистра (1,1,1) и (1,1,0), а также (0,1,1) и (0,1,0) даст всегда одно и тоже состояние регистра, а пара (1,0,1) и (1,0,0) разное независимо от других $a_{ij}=1 (j \neq L)$;

3) если $a_{13}=a_{23}=1$, то пара состояний регистра (1,0,1) и (1,0,0), а также (0,1,1) и (0,1,0) даст всегда одно и тоже состояние регистра, а пара (1,1,1) и (1,1,0) разное независимо от других $a_{ij}=1 (j \neq L)$.

Для наглядности сведем полученные данные в табл. 1.

Таблица 1

Комбинации состояний РСНОС второго порядка для $L=3$, которые будут давать одинаковые результирующие состояния в зависимости от наличия коэффициентов $a_{iL}=1$ и при любых других $a_{ij} (j \neq L)$

Состояния регистров a_{ij}	(1,0,0)	(0,1,0)	(1,1,0)
$a_{13}=1$	(1,0,1)		(1,1,1)
$a_{23}=1$		(0,1,1)	(1,1,1)
$a_{13}=a_{23}=1$	(1,0,1)	(0,1,1)	

Аналогичную сводную таблицу можно составить для $L=4$ (табл. 2), изучая все возможные

Таблица 2

Комбинации состояний РСНОС второго порядка для $L=4$, которые будут давать одинаковые результирующие состояния в зависимости от наличия коэффициентов $a_{iL}=1$ и при любых других $a_{ij} (j \neq L)$

Состояния регистров a_{ij}	(1,0,0,0)	(0,1,0,0)	(0,0,1,0)	(1,1,0,0)	(0,1,1,0)	(1,0,1,0)	(1,1,1,0)
$a_{14}=1$	(1,0,0,1)			(1,1,0,1)		(1,0,1,1)	(1,1,1,1)
$a_{24}=1$		(0,1,0,1)		(1,1,0,1)	(0,1,1,1)		(1,1,1,1)
$a_{34}=1$			(0,0,1,1)		(0,1,1,1)	(1,0,1,1)	(1,1,1,1)
$a_{14}=a_{24}=1$	(1,0,0,1)	(0,1,0,1)			(0,1,1,1)	(1,0,1,1)	
$a_{24}=a_{34}=1$		(0,1,0,1)	(0,0,1,1)	(1,1,0,1)		(1,0,1,1)	
$a_{14}=a_{34}=1$	(1,0,0,1)		(0,0,1,1)	(1,1,0,1)	(0,1,1,1)		
$a_{14}=a_{24}=a_{34}=1$	(1,0,0,1)	(0,1,0,1)	(0,0,1,1)				(1,1,1,1)

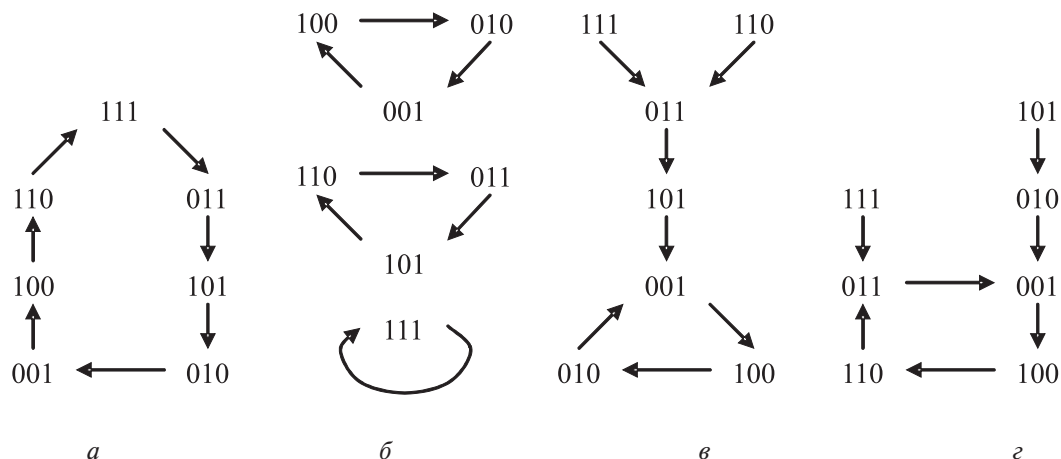


Рис. 4. Диаграмма состояний РСНОС второго порядка с образующими полиномами вида $a - (x^3 + x^1 + 1)$, $б - (x^3 + 1)$, $в - (x^3 + x^3x^2 + 1)$ и $з - (x^3 + x^3x^2 + x^2x^1 + x^1 + 1)$

(с учетом 1 требования) комбинации обратных связей второго порядка.

Таким образом, видим, что когда $a_{iL} = 1$, то соответствующие коэффициенты i состояний (т.е. $x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_{L-1}, 1$) всегда будут давать ноль независимо от других x_j ($j \neq i, L$). Результат также не будет зависеть и от других коэффициентов a_{ij} . Покажем это.

Рассмотрим, какие значения порождает фиксированная комбинация нелинейной связи вида $a_{iL} = 1, a_{LL} = 1$, что соответствует формульному виду $x^L + x^L x^i$:

x_i	x_L	$x^L + x^L x^i$
1	0	$0 + 0 \cdot 1 = 0$
1	1	$1 + 1 \cdot 1 = 0$

т.е. если $x_i = 1$, то независимо от x_L результат будет равен нулю, так как нелинейная комбинация будет компенсировать линейную составляющую.

Таким образом, как бы мы не изменяли параметры системы, т.е. a_{ij} ($j \neq L$) и x_j ($j \neq i, L$), то это может влиять только на результат (0 или 1) и ни как не зависят от x_L .

Теперь рассмотрим случай, когда две из всех возможных комбинаций $a_{iL} = 1$ ($i \in \{1, L-1\}$), пусть это будут комбинации $a_{kL} = a_{iL} = 1$, все остальные $a_{iL} = 0$. Тогда, если $x_k = 1$, а $x_i = 0$ (или $x_k = 0, x_i = 1$) будет случай, описанный выше. Когда $x_k = 1$ и $x_i = 1$, то при разных значениях x_L (0 или 1) будут генерироваться разные выходные значения. Действительно, если $x_L = 0$, то комбинация нелинейных слагаемых вида $x^L + x^L x^k + x^L x^i$ даст всегда ноль, а при $x_L = 1$ та же самая комбинация даст всегда 1. Обратим внимание, что это все изложенное выше не зависит от значения других a_{ij} и x_i .

Если рассмотреть случай, когда 3 коэффициента $a_{iL} = 1$ ($i \in \{1, L-1\}$), т.е. $x^L + x^L x^k + x^L x^i + x^L x^p$, тогда $(x_k = x_i = 0, x_p = 1)$, или $(x_k = x_p = 0, x_i = 1)$, или $(x_p = x_i = 0, x_k = 1)$, или $(x_k = x_i = x_p = 1)$ всегда даст результирующую сумму равную нулю независимо от значения x_L (0 или 1).

Обобщая, таким образом, полученные результаты, можно сформулировать в общем виде следующее правило для образования результирующего значения в сумме нелинейных комбинаций отдельных регистров.

Если $a_{LL} = a_{iL} = a_{jL} = a_{kL} = \dots = 1$ (i, j, k не равны между собой и $< L$) и им соответствует состояние регистров x_L, x_i, x_j, x_k , то:

– если $\sum_{i,j,k,\dots} x$ – нечетное число, то результат суммы $x^L + x^L x^i + x^L x^j + x^L x^k + \dots$ будет равен 0 независимо от значения x_L ;

– если $\sum_{i,j,k,\dots} x$ – четное число, то при $x_L = 0$ результат также равен 0, а при $x_L = 1$ результат равен 1.

Все вышеприведенное справедливо для любых других значениях x_i и a_{ij} .

Из приведенных на рис. 3 графиков можно увидеть определенную закономерность, которой подчиняются коэффициенты $a_{ij} = 1$ на всем множестве генерирующем максимальную последовательность (см. рис. 3 в, г), а также наблюдать симметрию по i относительно середины значений. Опираясь на выявленные требования, введем следующее понятие симметричного полинома.

Определение. Два полинома с максимальной степенью L будем называть *симметричными полиномами*, если они порождают симметричную последовательность. Т.е., если два полинома вырабатывают две различные последовательности Q_1 и Q_2 с периодом T , то для любой точки отсчета в последовательности Q_1 найдется точка отсчета в последовательности Q_2 , такая что при проходе справа налево (слева направо) для последовательности Q_1 она будет полностью идентична последовательности Q_2 при проходе слева направо (справа налево) на всем периоде T .

В табл. 3 приведено все множество a_{ij} для $L = 4$, при которых $T = T_{\max}$, с вырабатываемыми этими комбинациями последовательностями бит. Следует обратить внимание, что последовательности имеют идентичный вид, когда их проход осуществляется в обратном порядке (зеркальное отображение). Можно легко увидеть, что каждой комбинации a_{ij} соответствует симметричная a_{ij}^1 (например: $x^1 + x^1 x^2 + x^2 + x^4 \leftrightarrow x^2 + x^2 x^3 + x^3 + x^4$).

Получить коэффициенты РСНОС a_{ij}^1 , которые являются симметричными относительно коэффициентов РСНОС a_{ij} , можно с помощью следующего соотношения:

$$a_{ij}^1 = a_{(L-j)(L-i)} \quad (4)$$

Таблица 3

Полное множество коэффициентов обратной связи a_{ij} и их последовательности (Q) с максимальным периодом для РСНОС второго порядка при $L = 4$

$a_{11}a_{12}a_{13}a_{14}a_{22}a_{23}a_{24}a_{33}a_{34}a_{44}$	$Q(t) \rightarrow$	$a_{11}a_{12}a_{13}a_{14}a_{22}a_{23}a_{24}a_{33}a_{34}a_{44}$	$\leftarrow Q(t)$
100000001	111101011001000	000000101	000100110101111
110010001	111100101101000	0000110101	000101101001111
101010001	111100101000110	0010100101	011000101001111
011010001	111100110100010	0010110001	010001011001111
110010001	111100100011010	0100010101	010110001001111
1000110001	111101000110010	0100100101	010011000101111
1110110001	111101100101000	0110110101	000101001101111
1110100101	111101001011000	1010110101	000110100101111

Вернемся к коэффициентам обратной связи и рассмотрим их с точки зрения симметрии. В табл. 4 приведены коэффициенты a_{ij} для $L=4$ и симметричные им коэффициенты, которые генерируют последовательность максимального периода (табл. 4 справа) и остальные (табл. 4 слева), отвечающие требованиям 1-3.

Из табл. 4 видим, что некоторые комбинации симметричны сами к себе и что у таких комбинаций период меньше максимального. Такое утверждение верно и для $L=5, 6$ и 7 , рассчитанных без учета требований 1-3. Принимая это во внимание, можно сформулировать еще одно требование.

Требование 4. Полином на основе РСНОС второго порядка, который генерирует последовательность максимального периода, не должен быть симметричным сам к себе, т.е.:

$$a_{ij} \neq a_{(L-j)(L-i)}.$$

Количество полиномов в РСНОС второго порядка с максимальным периодом.

Обозначим через Λ_0 полное множество всех комбинаций значений, которые могут принимать коэффициенты обратных связей a_{ij} в РСНОС второго порядка. Так как a_{ij} может принимать только два значения, то справедливо:

$$\Lambda_0 = 2^{n_L}. \quad (5)$$

Λ_0 является достаточно большим числом даже для малых значений L (см. табл. 5), поэтому процесс нахождения всех полиномов РСНОС второго порядка генерирующие ПСП максимального периода (или оценка их количества) является очень трудоемким процессом. Учитывая полученные выше свойства, можно существенно уменьшить множество допустимых значений для a_{ij} . Обозначим через Λ множество допустимых значений a_{ij} , т.е. таких, которые удовлетворяют предъявляемым требованиям и могут генерировать ПСП с максимальным периодом. Выполнение первого требования приводит к сокращению множества искомых комбинаций в 2^1 раз, так как коэффициент a_{LL}

может принять только одно состояние. Если обозначить через Λ^1 множество комбинаций, которые не удовлетворяют 1 требованию, то его можно определить по следующей формуле

$$\Lambda^1 = 2^{n_L-1}. \quad (6)$$

Второе требование уменьшает оставшегося (и/или первоначальное) множества в 2^1 раза, так как сумма только каждой второй комбинации будет четной. Обозначив через Λ^2 множество комбинаций, не удовлетворяющих только 2 требованию, получаем

$$\Lambda^2 = 2^{n_L-1}. \quad (7)$$

Для определения количества полиномов, не удовлетворяющих третьему требованию (обозначим его через Λ^3), расположим коэффициенты обратных связей из (1) в виде квадратной матрицы (8):

$$\begin{matrix} a_{11} & a_{12} & a_{13} & \dots & a_{1L} \\ & a_{22} & a_{23} & \dots & a_{2L} \\ & & a_{33} & \dots & a_{3L} \\ & & & \dots & \\ & & & & a_{LL} \end{matrix} \quad (8)$$

Тогда все количество коэффициентов a_{ij} (n_L) можно разбить на две части: количество коэффициентов a_{iL} ($i \in \{1, L-1\}$) (число таких коэффициентов обозначим через $n^{3,1}$) и все множества остальных коэффициентов. В этом случае количество возможных комбинаций можно представить как произведения количества комбинаций из первого множества на количество комбинаций из второго множества, т.е.

$$\Lambda = \Lambda^{3,1} \cdot \Lambda^{3,2}, \quad (9)$$

где: $\Lambda^{3,1} = 2^{n^{3,1}}$ — множество комбинаций, составленных из коэффициентов первого множества; $\Lambda^{3,2} = 1$ — множество комбинаций, составленных из коэффициентов второго множества (так как, согласно 3 требованию, все $a_{iL} = a_{2L} = \dots = a_{(L-1)L} = 0$).

Таблица 4

Множество коэффициентов обратной связи a_{ij} для $L=4$, отвечающих требованиям 1-3, и периоды, которые генерируют с их помощью РСНОС второго порядка

a_{ij}	$a_{(L-j)(L-i)}$	T		a_{ij}	$a_{(L-j)(L-i)}$	T
111000001	0010010101	5		100000001	000000101	15
0100110001		5		1100100001	0000110101	15
1000100101		5		1010100001	0010100101	15
0000100001		6		0110100001	0010110001	15
0110010001		6		1100010001	0100010101	15
0010000001		7		1000110001	0100100101	15
1010000101		7		1110110001	0110110101	15
1110010101		7		1110100101	1010110101	15
1100110101		7				
0100000001	0000010001	9				
1010010001	0110000101	10				
1100000101	1000010101	10				

Количество коэффициентов в первом множестве можно определить аналогично (2), рассмотрев треугольник (8) без последнего столбца (что эквивалентно в (2) вместо L подставить $L-1$), но добавив коэффициент a_{LL} :

$$n^{3,1} = \frac{(L-1) \cdot (L-1+1)}{2} + 1 = \frac{L \cdot (L-1)}{2} + 1. \quad (10)$$

Таким образом, полное количество полиномов, не удовлетворяющих только 3 требованию, будет определяться как

$$\Lambda^3 = 2^{[n_L]} - 2^{\left[\frac{L \cdot (L-1)}{2} + 1\right]}. \quad (11)$$

Для определения множества полиномов, удовлетворяющих 1, 2 и 3 требованию, необходимо от всего множества возможных комбинаций Λ_0 вычесть те комбинации, которые не удовлетворяют выдвигаемым требованиям. Как пример полинома, не удовлетворяющего и 1 и 2 требованию, т.е. входящий в пересекаемое множество, можно привести полином степени 3 следующего вида: $x^1 + x^1 x^3 + x^2$. Для этого необходимо исключить пересекаемые части множеств, не удовлетворяющих требованиям 1-4. Обозначим через ${}^{-1}\Lambda^2$ множество комбинаций, не удовлетворяющих только 2 требованию и не пересекаемое с множеством комбинаций a_{ij} , отвергнутых 1 требованием. Из (6) и (7) такое множество определяется равенством:

$${}^{-1}\Lambda^2 = \frac{1}{2} \cdot \Lambda^2 = \frac{1}{2} \cdot 2^{n_L-1} = 2^{n_L-2}. \quad (12)$$

Для определения множества полиномов, не удовлетворяющих 3 требованию и не удовлетворяющих 1 и/или 2 требованиям (см. вышеприведенный пример), необходимо исключить пересекаемую часть. Обозначим через ${}^{-1,2}\Lambda^3$ множество

полиномов, не удовлетворяющих 3 требованию и соответствующих 1, 2 требованию. Из (8) нетрудно увидеть, что во множество (11) включен коэффициент a_{LL} (в соответствии с 1 требованием коэффициент a_{LL} принимает только одно значение), а сумма из половины оставшихся комбинаций коэффициентов будет четной. Таким образом, имеет место следующее равенство:

$${}^{-1,2}\Lambda^3 = \Lambda^3 / 4 = 2^{[n_L-2] - \left[\frac{L \cdot (L-1)}{2} - 1\right]}. \quad (13)$$

Из (6), (12) и (13) можно получить количество комбинаций коэффициентов a_{ij} , не удовлетворяющих 1, 2 и 3 требованию (обозначим это множество как Λ^{1-3}):

$$\begin{aligned} \Lambda^{1-3} &= \Lambda^1 + {}^{-1}\Lambda^2 + {}^{-1,2}\Lambda^3 = \\ &= 2^{[n_L]} - 2^{\left[\frac{L \cdot (L-1)}{2} - 1\right]} = \\ &= 2^{[n_L] - \left(1 - 2^{\left[\frac{L \cdot (L-1)}{2} - 1\right]}\right)}. \end{aligned} \quad (14)$$

Количество симметричных комбинаций a_{ij} обозначим его через Λ^4 , однозначно определяется длиной РСНОС (L). Зависимость значений Λ^4 от L можно определить, рассмотрев матрицу коэффициентов (8). Симметричными являются те комбинации a_{ij} , которые имеют осевую симметрию вдоль диагонали, идущей с правого верхнего угла (без учета столбца с коэффициентами a_{iL}) в нижний левый угол. Например, для $L=4$ все возможные варианты комбинаций коэффициентов 11, 12, 13, 22 имеют симметричные им коэффициенты 33, 23, 13, 22 (визуально это все коэффициенты по одну из сторон диагонали, включая саму диагональ

Таблица 5

Объединенные результаты вычислений для РСНОС второго порядка

	Длина РСНОС (L)				
	4	5	6	7	8
Количество коэффициентов обратных связей (n_L)	10	15	21	28	36
Максимально возможный период последовательности ($T_{\max}$)	15	31	63	127	255
Количество возможных комбинаций обратных связей второго порядка для РСНОС (Λ_0)	1 024	32 768	2 097 152	268 435 456	68 719 476 736
Количество допустимых (при $T = T_{\max}$) комбинаций обратных связей с учетом 1-4 свойств ($\Lambda_0 - \Lambda^{1-4}$)	24	480	16 128	1 046 528	134 184 960
$\frac{\Lambda_0 - \Lambda^{1-4}}{\Lambda_0} \cdot 100\%$	2,34%	1,46%	0,77%	0,39%	0,20%
Количества комбинаций обратных связей (при $T = T_{\max}$) полученное эмпирическим путем ($\Lambda_{\max}^1$)	16	128	2 048	65 536	4 194 304
Расчетное (экспериментальное) значение полиномов, период ПСП которых максимален ($\Lambda_{\max}$)	16	128	1 952	64 056	4 017 998

кроме столбца с коэффициентами a_{iL}) и составляют симметричные пары. Можно определить все коэффициенты, вариации которых будут обеспечивать набор симметричных коэффициентов, для любого L :

$$\Lambda^4 = 2^{n^4}, \quad (15)$$

где $n^4 = \frac{L^2}{4} + L$ — число коэффициентов, не удовлетворяющих 4 требованию для четных L ; $n^4 = \frac{L^2-1}{4} + L$ — число коэффициентов, не удовлетворяющих 4 требованию для нечетных L .

Пусть ${}^{-1,2,3}\Lambda^4$ будет множество комбинаций коэффициентов a_{ij} , не удовлетворяющие 4 требованию и не пересекаемые с множествами комбинаций, не удовлетворяющих требованиям 1-3. Требование 1 уменьшит Λ^4 в 2^1 раза, требование 2 также 2^1 раза, а требование 3 — в 2^{L-1} раз. Таким образом, ${}^{-1,2,3}\Lambda^4$ можно определить следующим равенством:

$${}^{-1,2,3}\Lambda^4 = {}^{-1,2}\Lambda^3 + \frac{\Lambda^4}{2^{L+1}}. \quad (16)$$

Таким образом, можно получить множество полиномов, не удовлетворяющих с 1 по 4 требованиям (Λ^{1-4}):

$$\Lambda^{1-4} = \Lambda^{1-3} + {}^{-1,2,3}\Lambda^4 = \begin{bmatrix} n_L \\ 2 \end{bmatrix} - 2 \begin{bmatrix} \frac{L \cdot (L-1)}{2} - 1 \\ -2 \end{bmatrix} + 2 \begin{bmatrix} n^4 \\ +2 \end{bmatrix}, \quad (17)$$

где $n^4 = \frac{L^2}{4} - 1$ — для четных L ; $n^4 = \frac{L^2-1}{4} - 1$ — для нечетных L .

Или же, если вынести коэффициент 2^{n^4} , уравнение (17) можно переписать в следующем виде:

$$\Lambda^{1-4} = 2^{n^4} \cdot \begin{pmatrix} n_L & -(L+1) & -n^4 \\ 1-2 & & +2 \end{pmatrix}, \quad (18)$$

где $n^4 = \left(\frac{L}{2}\right)^2 + \frac{L}{2} + 1$ — для четных L ; $n^4 = \left(\frac{L+1}{2}\right)^2 + 1$ — для нечетных L .

Определенный интерес имеет количественная оценка полученного результата. Из выражения (18) вычислим, в процентах, количество полиномов, которые удовлетворяют требованиям 1-4 по отношению ко всему множеству возможных комбинаций обратных связей в зависимости от L :

$$\frac{\Lambda_0 - \Lambda^{1-4}}{\Lambda_0} \cdot 100\% = \left(\frac{1}{2} \frac{1}{[L+1]} - \frac{1}{2} \frac{1}{[n^4]} \right) \cdot 100\%, \quad (19)$$

где n^4 принимают значения, указанные в (18).

С учетом вышеприведенного были проведены вычисления для $L = 1-8$, результаты которых приведены в табл. 5.

Из (19) видим, что процент полиномов, которые теоретически могут порождать ПСП с максимальным периодом, по отношению ко всему множеству полиномов, уменьшается по степенной зависимости при увеличении числа регистров в РСНОС второго порядка. В табл. 5 указано, что уже при $L=6$ количество таких полиномов меньше 1%. Также из (19) можно констатировать, что вклад 4 требования уменьшается по квадратичной зависимости с увеличением L .

Как видно из табл. 5, количество комбинаций a_{ij} , при которых $T = T_{\max}$ (обозначим её через $\Lambda_{\max}^1$) меньше значения Λ^{1-4} , полученного с помощью формулы (18), на несколько порядков.

Анализ полученных результатов позволяет предложить нам следующее эмпирическое выражение для $\Lambda_{\max}^1$:

$$\Lambda_{\max}^1 \leq 2^{\frac{L(L-1)}{2} - L + 2}. \quad (20)$$

Применение выражения (20) дает погрешность для $L = 8$ не выше 4,3%.

Необходимо заметить, что при поиске всех РСНОС второго порядка с максимальным периодом можно сократить количество исследуемых комбинаций ещё в 2 раза, реализуя 4 требование. Так, если найдена комбинация a_{ij} , которая дает последовательность с максимальным периодом, то из 4 требования получаем РСНОС второго порядка также с максимальным периодом, не затрачивая при этом дополнительных ресурсов на его исследование его периода.

ВЫВОДЫ

В данной статье сформулированы четыре требования, которые должны выполняться в РСНОС второго порядка генерирующих последовательность с максимальным периодом. Основываясь на сформулированных требованиях, проведена строгая оценка верхней границы количества возможных полиномов (17) или (18), для заданной длины РСНОС, которые будут генерировать ПСП с максимальным периодом.

Данный результат становится особенно актуален при нахождении полиномов с большим значением L , когда заранее невозможно предсказать будет ли период, наугад взятого полинома, максимальным, а также для оценки количества возможных таких решений при проектировании такого рода генераторов.

Таким образом, нам удалось значительно уменьшить множество комбинаций a_{ij} , при которых наша система будет генерировать последовательность с максимальным периодом (см. табл. 5). Это позволит существенно сократить время для построения криптостойких систем на базе РСНОС, в которых будет использоваться большое количество регистров (L). И еще более существ-

венную роль сыграет при криптоанализе подобных систем.

Как пример результативности сформулированных требований можно привести тот факт, что при нахождении всех РСНОС, с максимальной генерируемой последовательностью, для $L=6$ и полном переборе всех возможных значений было затрачено 5 часов 12 минут машинного времени (вычисления проводились на ЭВМ Pentium 4 1,6 ГГц). При введении в алгоритм поиска ограничений определенных только 1-3 требованиями, на такой точно поиск было затрачено примерно в 240 раз меньше машинного времени (всего 1 минута 18 секунд).

Литература.

- [1] *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. — М.: Кудиц-образ, 2001. — 368 с.
- [2] *T. Beth, F.C. Piper.* The stop-and-go generator, Proceeding Eurocrypt, Springer-Verlag Lecture Notes in Computer Science 1984 — nr.209.
- [3] *W.G. Chambers,* Clock-controlled shift-registers in binary sequence generators, IEEE Proceedings, 1988. — 135 с.
- [4] *A. Klapper, M. Goresky,* Large periods nearly de Bruijn FCSR sequences, Adv. In Cryptology EuroCrypt, 1995.
- [5] *Асосков А.В., Иванов М.А., Мирский А.А., Рузин А.В., Сланин А.В., Тютвин А.Н.* Поточные шифры. — М.: Кудиц-образ, 2003. — 336 с.
- [6] *R.A. Games, A.H. Cham.* A fast algorithm for determining the complexity of a binary sequence with period 2^n . IEEE Transactions on Information Theory, IT-29: 144-146, 1983.
- [7] *Иванов М.А., Чугунков И.В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей. — М.: Кудиц-образ, 2003. — 240 с.

Поступила в редколлегию 4.09.2008



Потий Александр Владимирович, доктор технических наук, доцент, доцент кафедры БИТ ХНУРЭ. Область научных интересов: проектирование и разработка средств КЗИ.

Полуяненко Николай Александрович, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: проектирование и разработка средств КЗИ.