УДК 004.056.55

ВЫБОР ОБРАЗУЮЩИХ ПОЛИНОМОВ ДЛЯ РЕГИСТРА СДВИГА С НЕЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ ВТОРОГО ПОРЯДКА ГЕНЕРИРУЮЩИХ ПОСЛЕДОВАТЕЛЬНОСТЬ С МАКСИМАЛЬНЫМ ПЕРИОДОМ

Александр Потий[1], Николай Полуяненко[2]

[1] Харьковский национальный университет имени В.Н. Каразина, площадь Свободы, 4, г. Харьков, 61022, Украина
potav@ua.fm

[2] Харьковский национальный университет радиоэлектроники, соискатель кафедры БИТ
rsnos@mail.ua

Рецензент: Виктор Долгов, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: dolgovvi@mail.ru

Поступила в феврале 2016

Аннотация. *Рассмотрена модель генератора псевдослучайной последовательности на основе регистров сдвига с нелинейной обратной связью второго порядка. Сформулированы дополнительные требования к виду полинома, ограничивающее множество полиномов при выборе генерирующего последовательность с максимальным периодом. Приведено выражение для определения количества полиномов, не удовлетворяющих сформулированным требованиям. Дана количественная оценка влияния каждого требования на отсекаемое множество полиномов. Сформулированы рекомендации по применению указанных требований.*

Ключевые слова: *поточные шифры, регистры сдвига, нелинейные системы.*

1 Введение

В настоящее время многие структуры генераторов поточных шифров (рис.1) основаны на идее синхронного, классического суммирующего генератора и принадлежат к классу схем с равномерным движением регистра. К таким структурам относятся: SNOW, SOBER (t16, t32, 128), TURING. Основными элементами таких структур, как правило, является регистр сдвига с линейной обратной связью (РСЛОС) и схема усложнения.

Надежные криптоалгоритмы основываются на принципе, в соответствии с которым, силовая атака (*т.е. атака, в основу которой положен полный перебор всех возможных комбинаций ключа*) должна быть наиболее эффективна по сравнению с остальными предлагаемыми видами атак (*аналитическими или статистическими*).

Рис. 1 – Общая модель структуры генераторов поточных шифров

Для усложнения выходной последовательности в структуру генератора поточных шифров вводится нелинейность. Существуют различные пути введения нелинейности [1]. В большинстве современных поточных шифров нелинейная функция вводиться на выходе генератора для усложнения выходной последовательности одного или нескольких линейных рекуррентных регистров сдвига.

Наряду с разнообразными подходами [2-4], одним из возможных способов усложнения является внесение нелинейности в саму рекуррентную последовательность, путем введения нелинейности в обратную связь регистров сдвига. Кроме того, в настоящее время важную роль играют системы генерации случайных чисел, основанные на регистрах сдвига с нелинейной обратной связью (РСНОС) [5]. Преимущество таких систем заключается в следующем:

– выходная последовательность имеет те же характеристики, что и хорошо изученные РСЛОС (*прохождение тестов на случайность генерируемой последовательности*);

– структура (объем памяти, количество операций на один выходной бит, архитектура производства) практически идентично РСЛОС;

– нелинейность уже введена в регистр, что не требует дополнительного усложнения (а как следствия, дополнительного объема оперативной памяти и дополнительных вычислительных операций), т.е. соотношения время/память аналогично РСЛОС;

– отсутствие простых алгоритмов для восстановления структуры РСНОС по генерируемой ими последовательности, таких как, например алгоритм Берлекэмпа-Мэсси для РСЛОС;

– простота в программной и аппаратной реализации;

– значительно большее количество комбинаций обратной связи при одинаковой длине регистра. Если у РСЛОС длины L количество всех возможных комбинаций обратных связей определяется как 2^L, то у РСНОС той же длины их будет $2^{\frac{L^2+L}{2}}$.

К недостаткам применения РСНОС следует отнести то, что на сегодняшний день даже такую простую характеристику, как период формируемой РСНОС гаммы, трудно определить.

На этапе проектирования и создания генератора случайных чисел основополагающим моментом является выбор образующего полинома РСНОС, который будет генерировать последовательность с максимально возможным периодом. В дальнейшем, последовательность, которая имеет максимально возможную длину, будем называть М-последовательностью, а образующие полиномы РСНОС, которые генерируют М-последовательности – М-полиномами.

Однако, утверждать, что случайным образом взятый полином является М-полиномом, не проведя соответствующую проверку генерируемой последовательности, невозможно. Для достаточно большой степени такого рода полиномов провести вычислительную проверку одной последовательности (с целью определения ее периода), является достаточно трудоемкой задачей. Причем, процент М-полиномов от всех возможных, уменьшается по степенной зависимости с увеличением степени полиномов и, следовательно, поиск хотя бы одного М-полинома (для высокой степени) представляет относительно сложную задачу.

В качестве примера можно привести следующие оценки. Для РСНОС длиной L=128 полное количество возможных РСНОС составляет 2^{8256}. При этом, пользуясь оценочной формулой из [6], часть полиномов, которые могут генерировать М-последовательность, будет составлять менее $3 \cdot 10^{-77}$ от общего количества возможных.

Целями данной статьи являются выработка рекомендаций, касающихся методики выбора М-полинома для РСНОС и обоснование точной количественной оценки верхней границы числа М-полиномов в зависимости от длины РСНОС.

2 Общая модель РСНОС второго порядка

Рассмотрим систему генерации псевдослучайной двоичной последовательности основанной на РСНОС. В качестве обратной связи будем использовать побитовое сложение (обозначенное знаком – $\oplus$) и нелинейную функцию – умножения (обозначенное знаком – $\otimes$). Через L обозначим количество ячеек в регистре сдвига На рис. 2 представлен пример изучаемой модели РСНОС при *L=4*.

В данном случае блок умножения определяет наличие обратной связи. Так, при $a_{ij}=1$ соответствует наличию связи, а при $a_{ij}=0$ - отсутствию такой связи. В общем случае обратную связь для такой системы можно задать в следующем виде:

$$q_1(t+1)=\sum_{i=1}^{L}\sum_{j=i}^{L}a_{ij}q_i(t)q_j(t), \quad (1)$$

где мы учитываем, что $q_i \cdot q_i = q_i$ (т.е. умножение значения регистра самого на себя не дает никакого изменения). Как следствие, на рис. 2 знак ⊗ между i и i регистром опущен.

При рассмотрении рис.2 следует учитывать следующие допущения и сокращения: $a_{ij} \in \{0,1\}$ - блок умножения; $q_i(t) \in \{0,1\}$ - значение i-ого регистра в момент времени t; ⊕ – знак суммы; ⊗ – знак умножения; Q – генерируемая последовательность (бит). Кроме того, коэффициенты a_{ij} будем считать *линейными коэффициентами*, если $i = j$ и, соответственно, *нелинейными коэффициентами* – если $i \neq j$.

Нелинейная функция (1) обратной связи состоит из суммы произведений двух регистров. Назовем такую нелинейность – нелинейностью второго порядка.

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 $a_{ij} \neq 0$. Тогда для РСНОС 2-го порядка n_L определяется однозначно для заданного L следующим выражением:

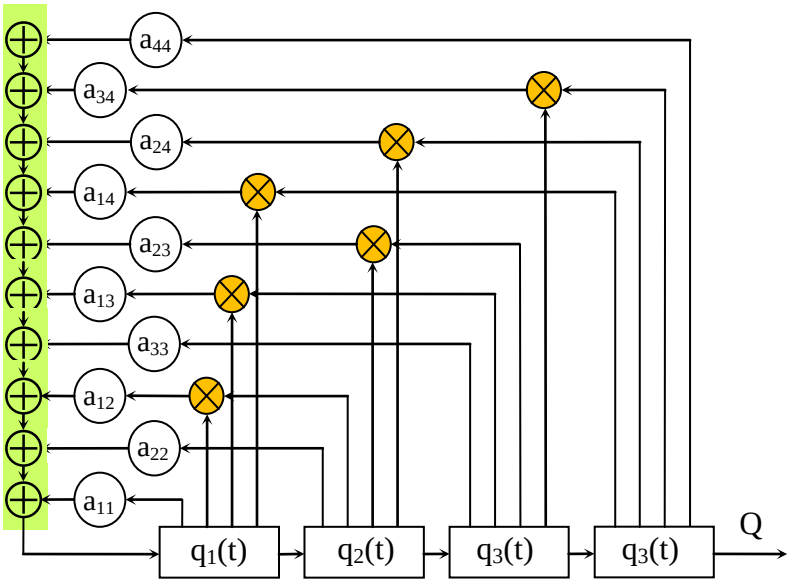

Рис. 2 – Общий вид генератора ПСП на РСНОС при $L=4$

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

Обозначим через Λ_0 полное множество всех комбинаций значений, которые могут принимать коэффициенты обратных связей a_{ij} в РСНОС второго порядка [6]:

$$\Lambda_0 = 2^{n_L}.$$

Заметим, что при использовании РСЛОС количество обратных связей, которыми можно варьировать, равно L (т.е. $n_L = L$) и $\Lambda_0 = 2^L$.

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

В работе [6] были сформулированы требования, которым должен отвечать полином генерирующий М-последовательность. Приведем их:

Требование 1. Для обеспечения максимального периода линейный коэффициент обратной связи от последнего регистра должен присутствовать всегда, т.е.: $a_{LL} = 1$.

Требование 2. Сумма всех ненулевых коэффициентов обратной связи a_{ij} должна быть четным числом, т.е.: $\sum_{i,j=1}^{L} a_{ij}$ - четное число.

Требование 3. Не должно быть нелинейной обратной связи, полученной от выходного регистра и любого другого регистра, т.е.: $\forall a_{iL} = 0, i = \overline{\{1, L-1\}}$.

Требование 4. Образующий полином РСНОС второго порядка, который генерирует М-последовательность, не должен быть симметричным сам к себе, т.е.: $a_{ij} \neq a_{(L-j)(L-i)}$.

Определение: Два полинома с максимальной степенью *L* будем называть *симметричными полиномами*, если РСНОС на их основе будут порождать симметричные последовательности. То есть, 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 чтении справа налево (слева направо) для последовательности Q_1 она будет полностью идентична последовательности Q_2 при чтении слева направо (справа налево) на всем периоде *T*.

Кроме того в работе [6] представлены выражения обеспечивающие подсчет количества полиномов, не удовлетворяющих указанным выше требованиям. Так, если через $\Lambda^{1,2,3,4}$ обозначить количество полиномов, не удовлетворяющих выше перечисленным требованиям, а через Λ^m обозначим количество полиномов, не удовлетворяющих m-му требованию, то это множество будет определяться следующими формулами:

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

$$\Lambda^4 = 2^{\left[\frac{L^2-k}{4}+L\right]}, \qquad \Lambda^{1,2,3,4} = 2^{[n_L]} \cdot \left(1 - 2^{-[L+1]}\right) + 2^{\left[\frac{L^2-k}{4}-1\right]}$$

где $k = 0$ – для четных L; $k = 1$ – для нечетных L.

Продолжим изучение полиномов и генерируемых на их основе последовательностей. Для этого рассмотрим ряд полиномов, у которых из всех слагаемых присутствует только одно линейное слагаемое (исходя из требования 1, это должно быть слагаемое наивысшего порядка, т.е. $a_{LL} = 1$) и любое количество нелинейных слагаемых. Для примера возьмем *L=4*, и рассмотрим полиномы вида:

$x^4 + x^2x^1 + 1$; $x^4 + x^3x^2 + 1$; $x^4 + x^3x^1 + x^2x^1 + 1$; $x^4 + x^4x^1 + x^3x^1 + x^2x^1 + 1$ и так далее.

Если изучить последовательности, которые генерируют такие полиномы при различных начальных состояниях, то можно увидеть, что из всего множества колец состояний, которые будут принимать регистры (и из всех возможных периодов *T*), во всех случаях будет иметь место одно и тоже кольцо состояний регистра ($1000 \to 0100 \to 0010 \to 0001 \to 1000$) с периодом равным длине РСНОС.

Перемножение двух любых ячеек такого регистра, при начальном заполнении ячеек регистра одной единицей и всеми нулями, дает в результате всегда ноль. Следовательно, любой РСНОС при рассмотренном начальном заполнении будет эквивалентен (*порождать идентичную последовательность*) полиному вида – $x^L + 1$. На основе вышеизложенного, сформулируем очередное требование.

Требование 5. У полинома на основе РСНОС второго порядка, который может генерировать последовательность максимального периода, должно быть больше одного ($a_{LL} = 1$ из требования 1) линейного коэффициента обратных связей, т.е.:

$$\sum_{i=1}^{L-1} a_{ii} \geq 1$$

Получим оценку количества РСНОС, которые не удовлетворяют требованию 5 и, следовательно, могут быть исключены из рассмотрения при поиске М-полинома только из анализа образующего полинома.

Обозначим через Λ^5 полное количество РСНОС длины L, которые не удовлетворяют требованию 5. Расположим коэффициенты обратных связей в виде матрицы

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

Тогда Λ^5 будет соответствовать множеству возможных комбинаций значений коэффициентов a_{ij}, исключая главную диагональ (*так как на ней расположены коэффициенты только линейной обратной связи*) и коэффициента a_{LL}. Число таких комбинаций составляет 2^{t+1}, где: t – количество коэффициентов нелинейных обратных связей; 2^1 – число вариаций с коэффициентом a_{LL}. Значение t можно определить из рассматриваемого треугольника (2)

$$\frac{L\cdot(L-1)}{2}.$$

Таким образом, полное количество РСНОС длины L, не удовлетворяющих требованию 5, будет равно:

$$\Lambda^5 = 2^{\frac{L\cdot(L-1)}{2}+1}.$$

Учитывая, что $n_L - L = \frac{L\cdot(L+1)}{2} - L = \frac{L\cdot(L-1)}{2}$, вышеприведенное равенство можно представить как:

$$\Lambda^5 = 2^{n_L-(L-1)}.$$

Следует подчеркнуть, что множество полиномов, которые не соответствуют требованию 5, пересекается с множеством полиномов, которые отсекаются требованиями 1-4.

Пусть Λ – общее количество допустимых полиномов, которые образуют РСНОС второго порядка, т.е. таких, которые из полного множества всех возможных полиномов удовлетворяют предъявляемым к ним требованиям и, следовательно, могут генерировать М-последовательности.

С учетом выдвинутых пяти требований Λ будет определяться по формуле:

$$\Lambda = 2^{\left\lfloor \frac{L\cdot(L-1)}{2}-1 \right\rfloor}\cdot\left(1-2^{[1-L]}\right) - 2^{\left\lfloor \frac{L^2-k}{4}-1 \right\rfloor}\cdot\left(1-2^{\left\lfloor \frac{k-L}{2} \right\rfloor}\right)$$

где $k=0$ – для четных L; $k=1$ – для нечетных L.

Оставшиеся РСНОС с $L=4$, отвечающие требованиям 1÷5, но не генерирующие М-последовательность, будут генерировать кольца вида $(1010)\rightarrow(0101)\rightarrow(1010)$. Формирование колец такого вида происходит при условии, что присутствующие линейные и нелинейные коэффициенты a_{ij}, в указанных состояниях, будут друг друга компенсировать. Например, коэффициенты вида: $\underline{\underline{1}}0\underline{\underline{1}}0\ 010\ 00\,1$; $\underline{\underline{1}}\underline{\underline{1}}0\ 000\ 00\,1$ и симметричные им $0\underline{\underline{1}}\underline{\underline{1}}0\ 000\ \underline{\underline{1}}0\,1$; $00\underline{\underline{1}}0\ 010\ \underline{\underline{1}}0\,1$ (здесь и далее при такой записи коэффициенты a_{ij} из выражения (1) будут представлены в линейной форме, т.е. – $a_{11}a_{12}a_{13}a_{14}\ a_{22}a_{23}a_{24}\ a_{33}a_{34}\ a_{44}$). Подчеркнутые комбинации, в указанных состояниях регистра, компенсируют друг друга. Причем, не важно, какие еще будут нелинейные комбинации, их сумма всегда (*в указанных состояниях*) даст ноль.

То же самое будет и при взаимном отсутствии подчеркнутых слагаемых. Компенсировать линейные обратные связи могут и линейные комбинации, как пример: $\underline{\underline{1}}100\,000\,\underline{\underline{1}}0\,1$; $\underline{\underline{1}}000\,010\,\underline{\underline{1}}0\,1$.

Для принятия регистрами исходного состояния необходимо, чтобы в результате второго такта на вход подавалась единица. Этого можно добиться, если только $a_{22}\neq 1$ и $a_{24}\neq 1$ или же $a_{22}=a_{24}=1$, при условии, что $a_{44}=1$ или же $a_{22}=1$ или $a_{24}=1$, при условии, что $a_{44}\neq 1$.

Рассмотрим вариант с L=5. В данном случае также будет присутствовать кольцо вида: $(10101)\rightarrow(01010)\rightarrow(10101)$. Но, в отличие от предыдущего случая, для получения такого кольца, необходимо, чтобы обратные связи в первом такте не компенсировали друг друга.

На втором такте, необходимым условием для повторения состояния РСНОС является наличие $a_{22}=1$ или $a_{44}=1$, или же нелинейного коэффициента $a_{24}=1$, а также последняя из возможных комбинаций, когда все $a_{22}=a_{44}=a_{24}=1$.

Полученный результат можно распространить и для более высоких значений L. На рис. 3 представлены коэффициенты для четного (L=6) и нечетного (L=7) количества регистров, а также аналогичные кольца с периодом $T=2$. В круглые скобки взяты те коэффициенты, которые могут изменить генерируемое значение на первом такте работы, а в квадратные – влияющие на выходное значение, только на втором такте. Остальные коэффициенты a_{ij} можно опустить из рассмотрения, так как на любом такте они будут давать ноль.

(a_{11})	a_{12}	(a_{13})	a_{14}	(a_{15})	a_{16}
	$[a_{22}]$	a_{23}	$[a_{24}]$	a_{25}	$[a_{26}]$
		(a_{33})	a_{34}	(a_{35})	a_{36}
			$[a_{44}]$	a_{45}	$[a_{46}]$
				(a_{55})	a_{56}
					$[a_{66}]$

а)

(a_{11})	a_{12}	(a_{13})	a_{14}	(a_{15})	a_{16}	(a_{17})
	$[a_{22}]$	a_{23}	$[a_{24}]$	a_{25}	$[a_{26}]$	a_{27}
		(a_{33})	a_{34}	(a_{35})	a_{36}	(a_{37})
			$[a_{44}]$	a_{45}	$[a_{46}]$	a_{47}
				(a_{55})	a_{56}	(a_{57})
					$[a_{66}]$	a_{67}
						(a_{77})

б)

$(101010)\rightarrow(010101)\rightarrow(101010)$

в)

$(1010101)\rightarrow(0101010)\rightarrow(1010101)$

г)

Рис. 3 – Коэффициенты обратных связей для L=6 (а), L=7 (б) и последовательности, генерирующие такие системы для L=6 (в) и L=7 (*г*)

Следует обратить внимание, что в круглые скобки взяты коэффициенты a_{ij} у которых индексы i и j являются нечетными числами, а в квадратных только те коэффициенты a_{ij} у которых индексы i и j являются четными числами. Таким образом, на основании выше изложенного, можно сформулировать следующее утверждение.

Требование 6. Необходимым условием образующего М-полинома РСНОС второго порядка является одновременное невыполнение следующей пары условий:

- четность количества коэффициентов $a_{ij}=1$, индексы i и j которых являются нечетными числами (на рис. 2 коэффициенты в круглых скобках);
- нечетность количества коэффициентов $a_{ij}=1$, индексы i и j которых являются четными числами (на рис. 2 коэффициенты в квадратных скобках), или то же самое в формульном выражении:

$$\sum_{i,j\in A} a_{ij}\begin{cases}\text{четное число, где } A \text{ все множество нечетных чисел от 1 до } L;\\ \text{нечетное число, где } A \text{ все множество четных чисел от 1 до } L.\end{cases}$$

Количество полиномов, удовлетворяющих требованию 6 можно получить, рассмотрев запись коэффициентов a_{ij} в матричном виде (рис. 3 (а) и (б)). Коэффициенты, взятые в круглые и квадратные скобки, если их взять по отдельности, образуют треугольник, эквивалентный исходному треугольнику, но со сторонами в два раза меньшими. Это позволяет получить методику для подсчета количества возможных комбинаций из указанных коэффициентов. Обозначим через Λ^6 количество комбинаций a_{ij}, которые не удовлетворяют требованию № 6. Тогда Λ^6 определяется как:

$$\Lambda^6 = 2^{\left\lfloor \frac{L\cdot(L+1)}{2}-2 \right\rfloor}.$$

Исключая пересекаемое множество полиномов одновременно не удовлетворяющее нескольким из вышеприведенных требований, получим выражение для точного подсчета количества полиномов, не удовлетворяющих требованиям с 1 по 6, для $L \geq 4$:

$$\Lambda^{1,2,3,4,5,6} = 2^{n_L-1} + \frac{1}{2}\cdot 2^{n_L-1} + \frac{1}{4}\cdot\left\{2^{n_L-(L-1)}\cdot(2^{L-1}-1) + \frac{1}{2^{L-1}}\cdot\left(2^{\frac{L^2-k}{4}+L} + 2^{n_L-(L-1)} + \right.\right.$$
$$\left.\left. + 2^{n_L-2} - \left\lfloor 2^{\frac{L^2-k}{4}+L-\frac{L-k}{2}} + k\cdot 2\cdot 2^{\frac{L^2-k}{4}+L-2} + 2^{n_L-L-1} - k\cdot 2\cdot 2^{\frac{L^2-k}{4}-\frac{L-k}{2}+L-2} \right\rfloor\right)\right\}, \quad (3)$$

где $k=0$, при L – четном; $k=1$, при L – нечетном.

Выражение (3) позволяет определить точное количественное значение числа полиномов, не отвечающих предъявленным к ним требованиям и, следовательно, не способных сгенерировать последовательность с максимальным периодом.

4 Количественная оценка полученных результатов

Таким образом, сформулированы еще два требования (5 и 6) к виду полиномов, которые дополнительно исключают полиномы, не являющиеся М-полиномами. Рассмотрим влияние каждого требования на алгоритм поиска М-полиномов.

Для ускорения расчетов имеет смысл оценить какую часть из всего множества можно исключить, проведя анализ вида образующего полинома РСНОС с точки зрения предъявленных требований, а также – в какой последовательности желательно проводить тестирование, чтобы повысить вероятность отсечки не М-полиномов на начальном этапе проверки.

На рис. 4 приведены расчетные значения полиномов: - полное множество возможных полиномов (Λ_0) для заданного L; - количество полиномов, которые удовлетворяют требованиям 1÷6 (т.е. $\Lambda_0 - \Lambda^{1,2,3,4,5,6}$) и могут потенциально генерировать М-последовательность; - количество полиномов которые генерируют последовательность максимальной длины (*установленное вычислительным путем*); - полное множество возможных полиномов для РСЛОС (*это частный случай РСНОС при котором все нелинейные коэффициенты обратных связей равны нулю*).

Представленные на рис. 4 данные позволяют качественно оценить множество полиномов, которые можно использовать в генераторах поточных шифров, а также обеспечивают возможность оценить тенденцию их увеличения с ростом L. В этой связи важно подчеркнуть, что при проектировании поточных шифров на основе РСНОС количество возможных вариантов образующих М-полиномов многократно превосходит количество возможных схем для РСЛОС (*включающих в себя даже не М-последовательности*) при одинаковых L.

Приведем число образующих полиномов РСНОС не удовлетворяющих всем вышеперечисленным требованиям. Для количественной оценки воспользуемся нормированными величинами. Полученные данные сведены в Таблицу 1 (*где Λ^m - множество полиномов, не удовлетворяющих одному из шести сформулированных требований; m - номер требования предъявляемого к виду полиному*).

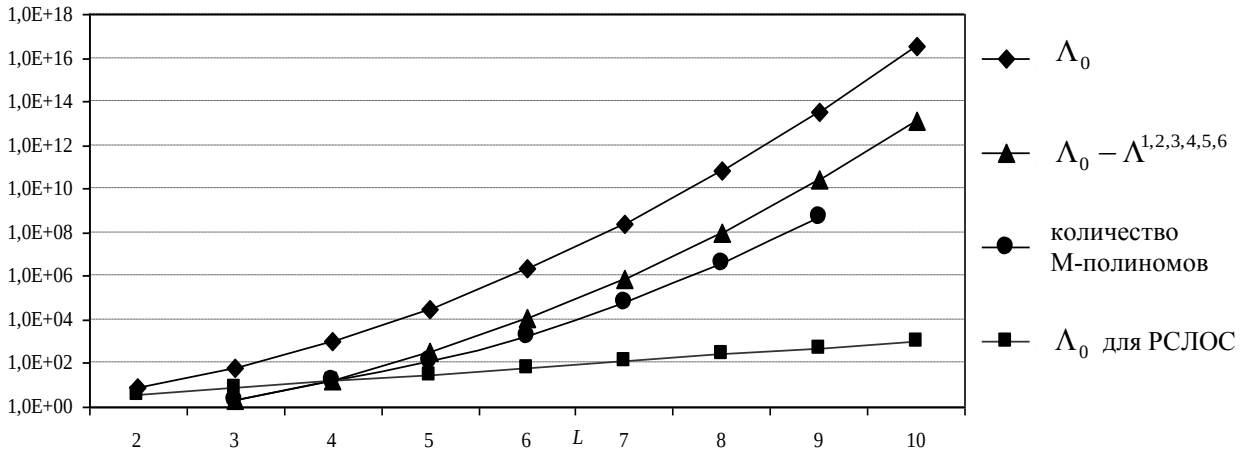

Рис. 4 – Количество полиномов в зависимости от длины РСНОС

Анализ данных таблицы позволяет утверждать, что при предъявлении к виду полинома требований 1÷6, уже при *L=10* отсекается порядка 99,9% от всего множества полиномов, причем с ростом значения *L (следует из (3))* этот процент растет по степенной зависимости.

Таблица 1 – Относительное количество полиномов, не удовлетворяющих требованиям 1÷6

L	Λ_0	$\frac{\Lambda^1}{\Lambda_0}$	$\frac{\Lambda^2}{\Lambda_0}$	$\frac{\Lambda^3}{\Lambda_0}$	$\frac{\Lambda^4}{\Lambda_0}$	$\frac{\Lambda^5}{\Lambda_0}$	$\frac{\Lambda^6}{\Lambda_0}$	$\frac{\Lambda^{1,2,3,4,5,6}}{\Lambda_0}$
2	8	0,5	0,5	0,5	1	0,5	0,25	1,000000
3	64	0,5	0,5	0,75	0,5	0,25	0,25	0,968750
4	1024	0,5	0,5	0,875	0,25	0,125	0,25	0,984375
5	32768	0,5	0,5	0,9375	0,0625	0,0625	0,25	0,989380
6	2097152	0,5	0,5	0,96875	0,015625	0,03125	0,25	0,994431
7	$2{,}7\cdot10^{8}$	0,5	0,5	0,984375	0,001953	0,015625	0,25	0,997119
8	$6{,}9\cdot10^{10}$	0,5	0,5	0,992188	0,000244	0,007813	0,25	0,998547
9	$3{,}5\cdot10^{13}$	0,5	0,5	0,996094	$1{,}5\cdot10^{-5}$	0,003906	0,25	0,999270
10	$3{,}6\cdot10^{16}$	0,5	0,5	0,998047	$9{,}5\cdot10^{-7}$	0,001953	0,25	0,999635
11	$7{,}4\cdot10^{19}$	0,5	0,5	0,999023	$3{,}0\cdot10^{-8}$	0,000977	0,25	0,999817
12	$3{,}0\cdot10^{23}$	0,5	0,5	0,999512	$9{,}3\cdot10^{-10}$	0,000488	0,25	0,999908
13	$2{,}5\cdot10^{27}$	0,5	0,5	0,999756	$1{,}5\cdot10^{-11}$	0,000244	0,25	0,999954
14	$4{,}1\cdot10^{31}$	0,5	0,5	0,999878	$2{,}3\cdot10^{-13}$	0,000122	0,25	0,999977

Кроме того из таблицы 1 следует, что максимальный вклад в отсечении полиномов, не генерирующих М-последовательность, дает требование № 3. Таким образом, при осуществлении поиска М-полиномов из всего множества возможных, для заданного *L*, необходимо в первую очередь проверять его на соответствие требованию № 3, а затем требованиям 1, 2 и 6. После этого осуществляется проверка требованию 5 и в последнюю очередь требованию 4.

В пользу указанного алгоритма выбора полиномов говорит тот факт, что проверку на соответствия требованиям № 3 и № 1 легко реализовать программным способом, при этом затрачиваемое машинное время – меньше, чем при проверке на соответствие требованиям №№ 2, 4 и 6.

Подводя итог вышесказанному, следует отметить следующее: - несмотря на малое количество полиномов, отсекаемых требованием № 4 *(по сравнению с требованием 3)*, им все же нельзя пренебрегать. Так, например, при больших значениях *L* требование 4 все равно отсекает достаточно большое множество не М-полиномов. При этом сложность при проверке с

помощью анализа генерируемой последовательности или другими известными способами, намного выше, чем анализ вида полинома.

В качестве примера приведем следующие расчеты: для $L=9$ число возможных полиномов $\Lambda_0 = 35\,184\,372\,088\,832$ (возьмем за 100%); требованием 3 отсекается 35 046 933 135 360 полиномов (что составляет 99,6%); остаток 137 438 953 472 полиномов (0,39%). При предъявлении к виду полиномов требований с 1 по 6 остается 25 668 894 720 полиномов (0,073%), что в 5,4 раза меньше, чем предыдущее число. При этом количество М-полиномов, полученных экспериментальным путем, будет всего 519 239 794, что составляет 0,0015% от общего множества или же 2% от множества полиномов соответствующих требованиям 1÷6.

Ссылки

[1] Ivanov M.A. Kriptograficheskie metody zashchity informatsii v komp'yuternykh sistemakh i setyakh / M.A. Ivanov . – Moskva: Kudits-obraz, 2001. – 368 s.
[2] Beth T. The stop-and-go generator, Proceeding Eurocrypt / T. Beth, F.C. Piper // Springer- Verlag Lecture Notes in Computer Science. – 1984 . – №209.
[3] Chambers W.G. Clock-controlled shift-registers in binary sequence generators / W.G. Chambers // IEEE Proceedings. – 1988. – 135 p.
[4] Klapper A. Large periods nearly de Bruijn FCSR sequences / A. Klapper, M. Goresky. – Cryptology EuroCrypt, 1995.
[5] Potochnye shifry / Asoskov A.V., Ivanov M.A., Mirskii A.A. i dr. – Moskva: Kudits-obraz, 2003. – 336 s.
[6] Potii A.V. Analiz svoistv registrov sdviga s nelineinoi obratnoi svyaz'yu vtorogo poryadka generiruyushchikh posledova-tel'nost' s maksimal'nym periodom / A.V. Potii, N.A. Poluyanenko // Prikladnaya radioelektronika. – 2008. – № 3. – S. 282-290.
[7] Stasev Yu.V., Potii A.V, Izbenko Yu.A. Issledovanie metodov kriptoanaliza potochnykh shifrov [Elektronnyi resurs]. – Rezhim dostupa: http://www.nrjetix.com/fileadmin/doc/publications/articles/stasev_potiy_izbenko_ru.pdf.

Reviewer: Viktor Dolgov, Doctor of Sciences (Engineering), Full Professor, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine. E-mail: dolgovvi@mail.ru

Received: February 2016.

Authors:
Oleksandr Potii, Doctor of Sciences (Engineering), Full Professor, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: potav@ua.fm
Nikolay Poluyanenko, applicant of the Department of ITS, Kharkiv National University of Radio Electronics. E-mail: rsnos@mail.ua

The selection of forming polynomials for shift register with nonlinear feedback second order that generates the sequence with maximum period.

Abstract. Model pseudo-random sequence generator based on shift registers with nonlinear feedback second order is considered. Additional requirements for type of polynomial are formulated. They limit the set of polynomials which generate a sequence with maximum period. The expression to determine the number of polynomials that do not meet the requirements is given. Quantitative estimation of the impact of each request on cuts the set of polynomials is given. Recommendations for the use of these requirements are formulated.

Keywords: stream ciphers, shift registers, nonlinear systems.

Рецензент: Віктор Долгов, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: dolgovvi@mail.ru

Надійшло: лютий 2016.

Автори:
Олександр Потій, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: potav@ua.fm
Микола Полуяненко, здобувач кафедри БІТ, Харківській національний університет радіоелектроніки. E-mail: rsnos@mail.ua

Вибір утворюючих поліномів для регістра зсуву з нелінійним зворотним зв'язком другого порядку, що генерують послідовність з максимальним періодом.

Анотація. Розглянуто модель генератора псевдовипадкової послідовності на основі регістрів зсуву з нелінійним зворотним зв'язком другого порядку. Сформульовано додаткові вимоги до виду полінома, що обмежують множену при виборі полінома, що генерує послідовність з максимальним періодом. Наведено вираз для визначення кількості поліномів, що не задовольняють наведеним вимогам. Надана кількісна оцінка впливу кожній з вимог на множену поліномів, що відсікається. Надані рекомендації щодо застосування зазначених вимог.

Ключові слова: потокові шифри, регістри зсуву, нелінійні системи.