УДК 004.056.55

ПОИСК РЕГИСТРОВ СДВИГА С НЕЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ, ФОРМИРУЮЩИХ ПОСЛЕДОВАТЕЛЬНОСТЬ МАКСИМАЛЬНОГО ПЕРИОДА

Н.А. ПОЛУЯНЕНКО

В статье рассматривается один из важных элементов генератора поточных шифров – регистры сдвига с нелинейной обратной связью (РСНОС). Рассмотрена проблема построения РСНОС, генерирующих последовательность максимального периода (М-последовательность). Дополняется ранее предложенный подход для поиска таких регистров. Показано, что с помощью предложенного подхода возможно исключить более 99% РСНОС, которые гарантированно не будут генерировать М-последовательность и тем самым значительно повысить скорость поиска РСНОС, генерирующих М-последовательность.

Ключевые слова: регистры сдвига с нелинейной обратной связью, М-последовательность, нелинейные полиномы, поточные шифры, псевдослучайные последовательности.

ВВЕДЕНИЕ

Информационная безопасность имеет первостепенное значение в современном мире для сферы управления и защиты государства, защиты коммерческой тайны и т.д. В настоящее время, большинство информации научного, финансового, юридического характера обрабатывается и хранится на компьютерах, а также взаимодействуют с другими компьютерами через открытую или незащищенную инфраструктуру. Многие из этих данных носят конфиденциальный характер.

Для того, чтобы защитить конфиденциальную информацию от несанкционированного или случайного доступа, как правило, применяют криптографические методы. Одним из наиболее распространенных подходов является использование псевдослучайной последовательности (ПСП), с помощью которой производят шифрование информации. Зашифрованная таким образом информация может быть восстановлена в первоначальное состояние только авторизованным пользователем.

В большинстве случаев, биты ПСП генерируются с помощью регистров сдвига с линейной обратной связью (РСЛОС). Преимуществом РСЛОС является простота реализации, высокая скорость и способность генерировать последовательность со статистическими характеристиками, как и случайная последовательность [1]. Кроме того, РСЛОС часто применяют для обнаружения и коррекции ошибок [2], сжатия данных [3], тестирования [4], а также в криптографии [5].

Распространенными криптографическими алгоритмами, которые построены с использованием РСЛОС, являются: поточный шифр A5/1, который используется для обеспечения конфиденциальности в телефонной сотовой связи стандарта GSM [6], поточный шифр E0, который используется в протоколе Bluetooth [7], и сжимающий генератор [8]. Основным недостатком РСЛОС является его линейность, которая приводит к относительно простому криптоанализу [9].

В качестве альтернативы РСЛОС для генерации ПСП в поточных шифрах были предложены регистры сдвига с нелинейной обратной связью (РСНОС). РСНОС на основе поточных шифров включаются в Achterbahn [10], Dragon [11], Grain [12], Trivium [13], VEST [14]. В работах [15, 16] показано, что РСНОС более устойчивы к криптоаналитическим атакам, чем РСЛОС. Вместе с тем, построение РСНОС большого размера с гарантированным периодом, остается нерешенной проблемой [17]. Только некоторые частные случаи были рассмотрены [18, 19, 20].

На сегодняшний день, наиболее полные и подробные работы по синтезу РСНОС, которые генерируют М-последовательности, представлены в работах [21, 22, 23, 24].

В данной статье продолжается работа по ранее предложенному подходу поиска РСНОС, гарантировано генерирующих ПСП максимальной длины (М-последовательность). В основе предложенного метода лежит анализ вида обратных связей в РСНОС и их взаимного расположения. Выдвигаются требования, невыполнение которых однозначно говорит о невозможности исследуемым РСНОС генерировать М-последовательность.

Общая модель РСНОС

Общая конструкция РСНОС для регистра, состоящего из $L = 4$ ячеек, приведена на рис. 1. В регистрах используется произведение только двух ячеек, и такие РСНОС назовем РСНОС второго порядка. В дальнейшем, под РСНОС понимаем РСНОС второго порядка в $GF(2)$.

На рис. 1 введены следующие обозначения: $a_{ij} \in \{0,1\}$ – коэффициент обратной связи, соответствует наличию или отсутствию обратной связи от произведения i-й и j-й ячейки регистра; $q_i(t) \in \{0,1\}$ – значение i-го регистра в момент времени t; Q – генерируемая последовательность бит.

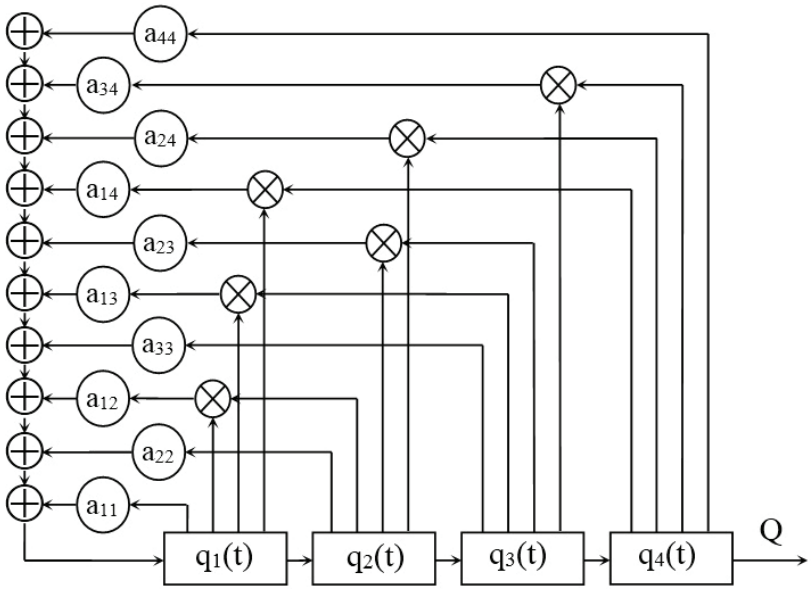

Рис. 1. Общая конструкция РСНОС

Знаком ⊗ обозначена нелинейная функция умножение, а ⊕ – линейная функция сложения.

Для удобства рассмотрения и восприятия обозначений коэффициентов обратной связи a_{ij} в РСНОС, отобразим их в виде матрицы:

$$\begin{array}{ccccc} a_{11} & a_{12} & a_{13} & \dots & a_{1L} \\ & a_{22} & a_{23} & \dots & a_{2L} \\ & & a_{33} & \dots & a_{3L} \\ & & & \dots & \dots \\ & & & & a_{LL} \end{array}$$

При этом диагональные элементы, т. е. a_{ii}, соответствуют частному случаю – РСЛОС.

В дополнение к восьми ранее изложенным Требованиям, описанным в [25, 26, 27], можно сформулировать следующее требование.

Описание Требования При рассмотрении всего множества последовательностей, которые могут генерировать РСНОС, обязательно будут присутствовать кольца с периодами меньше максимально возможного. Если исключить все кольца с периодом меньше $T_{\max} = 2^L - 1$, исключая соответствующие им комбинации a_{ij}, то останется только множество последовательностей (с соответствующими a_{ij}), которое будет являться М-последовательностью. Таким образом, для нахождения множества комбинаций a_{ij} генерирующих М-последовательность необходимо и достаточно определить и исключить все множество комбинаций a_{ij}, генерирующих последовательность с периодами T принадлежащим интервалу $1 \le T < T_{\max}$.

Для определенности скажем, что каждая последовательность в периоде будет начинаться с 1 и соответственно заканчиваться 0. Следующая за финальным нулем единица будет началом очередного периода. Это определение имеет одно исключение, когда $T = 1$, в этом случае последовательность в периоде будет состоять из одной 1 (и соответственно заканчиваться тоже 1).

В общем случае, при введенной системе обозначений (см. рис. 1), обратную связь для РСНОС, в момент времени t, можно задать в следующем виде:

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

а генерируемую при этом последовательность:

$$Q = \{q_1(t), q_1(t+1), q_1(t+2), \dots, q_1(t+i)\}.$$

Очевидно, что состояние i-й ячейки регистра в момент времени t соответствует генерируемому РСНОС значению в момент времени $t - i$. Следовательно, все состояния ячеек регистра определяется $q_i(t) = q_1(t+1-i)$.

Сгенерированная последовательность с периодом T записывается в виде:

$$Q_T = q_{i+1}, q_{i+2}, q_{i+3}, \dots, q_{i+T}, q_{i+1}, \dots.$$

При использовании приведенных обозначений, состояние регистра из L ячеек, генерирующего последовательность с периодом T, можно записать как:

$$[q_{i+1}, q_{i+2}, q_{i+3}, \ldots, q_{i+T}, q_{i+1}, \ldots, q_{i+L}]$$

при $T < L$;

$[q_{i+1}, q_{i+2}, q_{i+3}, \ldots, q_L]$ при $T \geq L$.

Таким образом, множество комбинаций состояний ячеек в регистре, или, что эквивалентно этому – генерируемой последовательности, можно разбить на подмножества состояний, соответствующих определенным периодам. В качестве примера запишем все возможные последовательности с $T < T_{\max}$ для $L = 3$ ($T_{\max} = 2^3 - 1 = 7$), сгруппировав их в соответствии с периодами:

$T = 1$	$T = 4$	$T = 5$	$T = 6$
$Q^1_{T=1} = \underline{1}111111$	$Q^1_{T=4} = \underline{1000}100$	$Q^1_{T=5} = \underline{1000}010$	$Q^1_{T=6} = 1000001$
$T = 2$	$Q^2_{T=4} = \underline{1100}110$	$Q^2_{T=5} = \underline{1100}011$	$Q^2_{T=6} = 1100001$
$Q^1_{T=2} = \underline{10}10101$	$Q^3_{T=4} = \underline{1010}101$	$Q^3_{T=5} = \underline{1010}010$	$Q^3_{T=6} = 1010001$
$T = 3$	$Q^4_{T=4} = \underline{1110}111$	$Q^4_{T=5} = \underline{1110}011$	$Q^4_{T=6} = 1110001$
$Q^1_{T=3} = \underline{100}1001$		$Q^5_{T=5} = \underline{1001}010$	$Q^5_{T=6} = 1001001$
$Q^2_{T=3} = \underline{110}1101$		$Q^6_{T=5} = \underline{1101}011$	$Q^6_{T=6} = 1101001$
		$Q^7_{T=5} = \underline{1011}010$	$Q^7_{T=6} = 1011001$
		$Q^8_{T=5} = \underline{1111}011$	$Q^8_{T=6} = 1111001$
			$Q^9_{T=6} = 1000101$
			$Q^{10}_{T=6} = 1100101$
			$Q^{11}_{T=6} = 1010101$
			$Q^{12}_{T=6} = 1110101$
			$Q^{13}_{T=6} = 1001101$
			$Q^{14}_{T=6} = 1101101$
			$Q^{15}_{T=6} = 1011101$
			$Q^{16}_{T=6} = 1111101$

Условием, при котором какой-либо из периодов будет повторяться, является генерация регистром значения $q_i = q_{i+T}$ для всех $i = 1, \ldots, T$. Если регистр, взятый с произвольными коэффициентами обратных связей a_{ij}, удовлетворяет вышеприведенному условию, то можно однозначно утверждать, что такой регистр генерирует кольцо с периодом T.

Задавая определенные состояния ячеек, проверяем, какое значение генерирует регистр при выбранных коэффициентах обратных связей. Проверку выполняем с помощью соответствующих *шаблонов*. Обозначим шаблон как $S_T^{r/k}$, где k порядковый номер шаблона в r-й последовательности для заданного проверяемого периода T.

Составим шаблоны каждой из итераций в последовательностях приведенного выше примера.

Для $T = 1$:

$$S^{1/1}_{T=1} = \begin{matrix} a_{11} = 1 & a_{12} = 1 & a_{13} = 1 \\ & a_{22} = 1 & a_{23} = 1 \Rightarrow 1 \\ & & a_{33} = 1 \end{matrix}$$

Под $a_{ij} = 1$ понимаем значимый коэффициент a_{ij}, т. е. такой коэффициент, значение которого влия-

ет на формирование выходного бита. Если $a_{ij}=0$, то указанный коэффициент не является значимым, т. е. не оказывает влияние на формирование выходного значения. Под обозначением «$\Rightarrow 1$» понимаем, что шаблон должен сгенерировать 1 или, что эквивалентно этому, сумма всех значимых коэффициентов a_{ij} должно быть число нечетное. Если «$\Rightarrow 0$», то шаблон должен сгенерировать 1, что эквивалентно четной сумме всех значимых коэффициентов a_{ij}.

Учитывая введенные обозначения, приведем шаблоны для $T=2$:

$$S^{1/1}_{T=2}=\begin{matrix}1&0&1\\0&0&\Rightarrow 0\\&1&\end{matrix}\quad S^{1/2}_{T=2}=\begin{matrix}0&0&0\\1&0&\Rightarrow 1\\&0&\end{matrix}$$

Таким образом, если в РСНОС одновременно выполняется условие для шаблона $S^{1/1}_{T=2}$ и $S^{1/2}_{T=2}$ (т. е., четность суммы коэффициентов $a_{11}+a_{13}+a_{33}$ и нечетность коэффициента a_{22}, а учитывая, что он единственный, то, следовательно $a_{22}=1$) является необходимым и достаточным условием для формирования РСНОС длины $L=3$ последовательности $Q=10101010\ldots$.

Шаблоны для $T=3$ имеют вид:

$$S^{1/1}_{T=3}=\begin{matrix}1&0&0\\0&0&\Rightarrow 0\\&0&\end{matrix}\quad S^{1/2}_{T=3}=\begin{matrix}0&0&0\\1&0&\Rightarrow 0\\&0&\end{matrix}$$

$$S^{1/3}_{T=3}=\begin{matrix}0&0&0\\0&0&\Rightarrow 1\\&1&\end{matrix}$$

$$S^{2/1}_{T=3}=\begin{matrix}1&1&0\\1&0&\Rightarrow 0\\&0&\end{matrix}\quad S^{2/2}_{T=3}=\begin{matrix}0&0&0\\1&1&\Rightarrow 1\\&1&\end{matrix}$$

$$S^{2/3}_{T=3}=\begin{matrix}1&0&1\\0&0&\Rightarrow 1\\&1&\end{matrix}$$

Шаблоны для $T=4$ имеют вид:

$$S^{1/1}_{T=4}=\begin{matrix}1&0&0\\0&0&\Rightarrow 0\\&0&\end{matrix}\quad S^{1/2}_{T=4}=\begin{matrix}0&0&0\\1&0&\Rightarrow 0\\&0&\end{matrix}$$

$$S^{1/3}_{T=4}=\begin{matrix}0&0&0\\0&0&\Rightarrow 0\\&1&\end{matrix}\quad S^{1/4}_{T=4}=\begin{matrix}0&0&0\\0&0&\Rightarrow 1\\&0&\end{matrix}$$

$$S^{2/1}_{T=4}=\begin{matrix}1&1&0\\1&0&\Rightarrow 0\\&0&\end{matrix}\quad S^{2/2}_{T=4}=\begin{matrix}0&0&0\\1&1&\Rightarrow 0\\&1&\end{matrix}$$

$$S^{2/3}_{T=4}=\begin{matrix}0&0&0\\0&0&\Rightarrow 1\\&1&\end{matrix}\quad S^{2/4}_{T=4}=\begin{matrix}1&0&0\\0&0&\Rightarrow 1\\&0&\end{matrix}$$

$$S^{3/1}_{T=4}=\begin{matrix}1&0&1\\0&0&\Rightarrow 0\\&1&\end{matrix}\quad S^{3/2}_{T=4}=\begin{matrix}0&0&0\\1&0&\Rightarrow 1\\&0&\end{matrix}$$

$$S^{3/3}_{T=4}=\begin{matrix}1&0&1\\0&0&\Rightarrow 0\\&1&\end{matrix}\quad S^{3/4}_{T=4}=\begin{matrix}0&0&0\\1&0&\Rightarrow 1\\&0&\end{matrix}$$

$$S^{4/1}_{T=4}=\begin{matrix}1&1&1\\1&1&\Rightarrow 0\\&1&\end{matrix}\quad S^{4/2}_{T=4}=\begin{matrix}0&0&0\\1&1&\Rightarrow 1\\&1&\end{matrix}$$

$$S^{4/3}_{T=4}=\begin{matrix}1&0&1\\0&0&\Rightarrow 1\\&1&\end{matrix}\quad S^{4/4}_{T=4}=\begin{matrix}1&1&0\\1&0&\Rightarrow 1\\&0&\end{matrix}$$

Заметим, что шаблоны $S^{1/k}_{T=4}$ и соответствующая им последовательность $Q=10001000\ldots$ физически не может быть реализована согласно конструкции РСНОС. Так как заполнение нулями всех регистров есть состояние запрещенное, и не может ни при каких коэффициентах a_{ij} образовать на выходе 1.

Также обратим внимание, что последовательность $Q^{3}_{T=4}$ и соответствующие ей шаблоны $S^{3/k}_{T=4}$ на самом деле являются суммой двух подпериодов $Q^{1}_{T=2}$ и соответствуют шаблонам $S^{1/1}_{T=2}$ и $S^{1/2}_{T=2}$.

Шаблоны для остальных периодов строятся аналогично вышеприведенным. Среди остальных шаблонов также присутствуют шаблоны и соответствующие им последовательности, которые либо не могут быть реализованы из-за особенности конструкции РСНОС, либо их можно представить в виде других периодов.

Можно воспользоваться альтернативным вариантом. Составить шаблоны только для последователь-

ностей максимального периода и проверим РСНОС на соответствие этим шаблонам. Однако, данный подход эквивалентен построению последовательности де Брейна и на практики, при больших значениях L, труднореализуем.

Обобщая вышеизложенный пример, видим, что для того чтобы отсеять все возможные комбинации коэффициентов обратных связей для $L=3$, которые будут генерировать последовательности с периодами меньшими максимально возможного, необходимо проанализировать вид РСНОС на соответствие девяти шаблонам. Или же составить и проанализировать два набора шаблонов для максимального периода.

Для больших значений L, начиная примерно с $L=15$, работа с массивом шаблонов для $T=T_{\max}$ является задачей, труднореализуемой для персональных компьютеров, использующих только данный метод. Причем, затрачиваемое время на проверку шаблонов, значительно превосходит время, затрачиваемое на проверку периода самой сгенерированной последовательности.

Количественная оценка применение Требований

Для РСНОС $L=7$ общее количество возможных комбинаций a_{ij} составляет 268 435 455. Общее количество комбинаций a_{ij}, которое не соответствует Требование 9 при $T=1,\ldots,L$ – 231 569 191 (86%). Оставшиеся комбинации (то есть те, которые удовлетворяют Требованию 9 при введенных ограничениях на размер тестируемого периода) – 36 866 264 (13,7%). Дополнительно применяя Требования 1, 3, 5 и 7, описанные в [25, 26, 27], сокращает оставшееся множество до 297 454 комбинаций, что соответствует 0,11% от общего множества.

С увеличением размера тестируемого периода, число полиномов, которые не прошли Требование 9, значительно уменьшается. С увеличением размера тестируемого периода также пропорционально увеличивается число шаблонов, которое необходимо протестировать, что увеличивает время на проверку тестируемого периода. Это позволяет нам обосновать очередность проверок шаблонов: от меньшего к большему значению T.

Проверочные шаблоны Требования 9 достаточно определить один раз для заданного L, после чего их можно применять при проверках для всех комбинаций коэффициентов a_{ij}.

Оценка затрачиваемых ресурсов

Количество возможных периодов для заданного L (обозначим через i_L) состоит из суммы всевозможных наборов периодов $T=1,2,\ldots,L$ (обозначим число таких вариантов для отдельно взятого T через i_T). Соответствующее для каждого периода количество шаблонов (обозначим как i_{TS}) возрастает с ростом L. Оценим верхнюю границу этого количества.

По определению, первым значением в периоде должна быть 1, а последним 0. Следовательно, эти элементы будут фиксированы, а все остальные могут принимать любые значения. Откуда получаем, что максимальное возможное число для заданного T, будет определяться соотношением:

$$i_T \le 2^{T-2}.$$

Заметим, что период $T=1,2$ являются исключением. В обоих случаях возможен лишь один период, это последовательность равная $q_1=1$ (для $T=1$) и $q_1=1, q_2=0$ (для $T=2$). В результате чего, количество возможных периодов, для заданного L, может быть подсчитано следующим соотношением:

$$i_L=\sum_{k=1}^{L} i_{T=k}.$$

При проверке на возможность РСНОС генерировать какой-либо из тестируемых периодов, следует проверить все возможные комбинации, которые будут обеспечивать создание заданного кольца. Количество шаблонов соответствует значению проверяемого периода, то есть:

$$i_{TS}=T.$$

Таким образом, полное количество шаблонов (обозначим как S_i), которые необходимо проверять при проверке РСНОС на соответствие Требованию 9, можно определить по формуле:

$$S_i=1_{(k=1)}+2_{(k=2)}+\sum_{k=3}^{L}\left(k\cdot 2^{k-2}\right)$$

При программной реализации, размещая все шаблоны в одном массиве, размерность массива будет $2^{L-2}\cdot L\cdot(n_L+1)$, где $n_L=L\cdot(L+1)/2$ число различных коэффициентов a_{ij}. К значению n_L добавлена 1, т. к. для каждого шаблона необходимо запоминать какое число он должен генерировать, 1 или 0.

Как видим, размерность данного массива возрастает с ростом L по степенной зависимости и уже при $L=20$ измеряется в Гбайтах, что является пробле-

мой при реализации на персональных компьютерах из-за ограничения оперативной памяти.

Введение различного рода оптимизаций в алгоритм позволяет существенно уменьшить объем затраченной памяти для проверки каждого периода, но не общую тенденцию роста затрачиваемых ресурсов.

Оценка временных затрат

В таблице 1 приведено время, затрачиваемое на проверку всего множества различных комбинаций a_{ij} в зависимости от числа взятых для проверки периодов и, соответственно, числа шаблонов, для различных значений L. Результат приведен без проверки самих комбинаций на генерацию М-последовательности. В таблице 2 указано время, затраченное на аналогичные тесты, но с проверкой на генерацию М-последовательностей.

Из результатов, приведенных в таблицах 1 и 2 можно сделать следующие выводы:

1. Подтверждается ранее приведенный результат, что с увеличением размера регистра увеличивается время на проверку в соответствии с Требованием 9 по степенному закону.

2. Многие из комбинаций коэффициентов a_{ij}, для отдельно взятого периода проверяемого кольца, дают также кольца, но с меньшим периодом. Это объясняет то, что время, затраченное на проверку шаблонов только для $T = 8$ (при $L = 8$) превосходит в 1.2 раза время, затраченное на проверку шаблонов с $T = 2 - 8$ и говорит в пользу очередности проведения проверок, начиная с меньших значений T.

3. Увеличение объема тестируемых периодов не приводит к сокращению затраченного времени на поиск М-РСНОС. При тестировании, для каждого L, существует оптимальное значение T. Для $L = 7$ оптимальный период находится в пределах $T = 2 - 5$, для $L = 8$ в пределах $T = 2 - 6$ и для $L = 9$ – при $T = 2 - 7$. С ростом числа проверяемых периодов с одной стороны уменьшается число комбинаций, которое необходимо проверить на генерацию М-последовательности. С другой стороны увеличивается число шаблонов и, соответственно, время на их проверку, что и приводит к увеличению общего затраченного времени.

Таблица 1

Тестируемые T	Затраченное время (сек.)					
	$L = 4$	$L = 5$	$L = 6$	$L = 7$	$L = 8$	$L = 9$ [1])
0	<0.01	<0.01	<0.01	0.2813	38.7969	10 375
2	<0.01	<0.01	<0.01	0.3750	47.5313	12 750
3	<0.01	<0.01	<0.01	0.4063	59.4531	16 600
2-3	<0.01	<0.01	<0.01	0.4375	60.1719	16 559
4	<0.01	<0.01	<0.01	0.5000	68.4844	18 150
2-4	<0.01	<0.01	<0.01	0.5469	77.3125	21 949
5		<0.01	<0.01	0.7343	103.313	28 243
2-5		<0.01	<0.01	0.8438	112.375	31 942
6			<0.01	0.9219	137.063	38 658
2-6			0.0156	1.0781	156.906	44 493
7				1.4375	202.031	61 683
2-7				1.5469	219.219	62 335
8					361.078	102 751
2-8					296.984	95 796
9						186 261
2-9						143 883

[1)] оценочное время, полученное прогнозированием.

Таблица 2

Тестирование вместе с генерацией гаммы и определением ее периода											
Тестируемые T	$L = 4$		$L = 5$		$L = 6$		$L = 7$		$L = 8$		$L = 9$ [1)]
	Протестировано комбинаций	Затраченное время (сек.)	Протестировано комбинаций	Затраченное время (сек.)	Протестировано комбинаций	Затраченное время (сек.)	Протестировано комбинаций	Затраченное время (сек.)	Протестировано комбинаций	Затраченное время (сек.)	Затраченное время (сек.)
2-4	16	<0.01	208	<0.01	7 216	0.047	463 680	3.438			
2-5			184	0.016	6 039	0.047	386 444	3.250	49 915 956	701.84	343 301
2-6					984	0.047	337 093	3.484	43 618 366	675.47	322 810

Продолжение таблицы 2

2-7							297 454	3.609	38 011 514	694.98	309 319
2-8									34 169 520	763.52	320 032
2-9											345 337

[1)] оценочное время, полученное прогнозированием.

ЗАКЛЮЧЕНИЕ

Применение Требования 9 при анализе вида и взаимного расположения коэффициентов обратных связей a_{ij} в РСНОС позволяет, теоретически, исключить все регистры, не генерирующие М-последовательность. Объем исключаемых РСНОС ограничен объемом используемой памяти и затрачиваемым временем.

Совместное использование Требования 9 с другими Требованиями позволяет значительно сократить, затрачиваемые на вычисления ресурсы и увеличить процент отсекаемого множества РСНОС не генерирующий М-последовательность. Для $L = 7$ проверка вида a_{ij} на соответствие Требованиям 1, 2, 5, 7 и Требование 9, при ограничении тестируемого периода $T = 1,\ldots,L$, позволила исключить из рассмотрения 99,89% РСНОС которые гарантированно не будут генерировать М-последовательность.

Практическая значимость представленной методики состоит в том, что она делает возможным сокращение исследуемого множества РСНОС, исключив регистры, не генерирующие М-последовательность, и тем самым повысить скорость поиска М-РСНОС.

Литература

[1] *S. Golomb*, Shift Register Sequences. Aegean Park Press, 1982.

[2] *J. McCluskey*, “High speed calculation of cyclic redundancy codes,” in Proceedings of the 1999 ACM/SIGDA seventh international symposium on Field programmable gate arrays, FPGA ’99, (New York, NY, USA), pp. 250–256, ACM, 1999.

[3] *G. Mrugalski, J. Rajski, and J. Tyszer*, “Ring generators - New devices for embedded test applications,” Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 23, no. 9, pp. 1306–1320, 2004.

[4] *R. David*, Random Testing of Digital Circuits. New York: Marcel Dekker, 1998.

[5] *S. Mukhopadhyay and P. Sarkar,* “Application of LFSRs for parallel sequence generation in cryptologic algorithms,” in Computational Science and Its Applications - ICCSA 2006, vol. 3982 of Lecture Notes in Computer Science, pp. 436–445, Springer Berlin / Heidelberg, 2006.

[6] *E. Biham and O. Dunkelman,* “Cryptanalysis of the A5/1 GSM stream cipher,” in INDOCRYPT ’00: Proceedings of the First International Conference on Progress in Cryptology, (London, UK), pp. 43–51, Springer-Verlag, 2000.

[7] *O. Y. Shaked*, “Cryptanalysis of the Bluetooth E0 cipher,” citeseer.ist.psu.edu/744254.html.

[8] *D. Coppersmith*, *H. Krawczyk, and Y. Mansour*, “The shrinking generator,” in CRYPTO ’93: Proceedings of the 13th annual international cryptology conference on Advances in cryptology, (New York, NY, USA), pp. 22–39, Springer-Verlag New York, Inc., 1994.

[9] *B. Schneier*, “A self-study course in block-cipher cryptanalysis,” Cryptologia, vol. XXIV, no. 1, pp. 18–33, 2000.

[10] *B. Gammel, R. Gottfert, and O. Kniffler,* “Achterbahn-128/80: Design and analysis,” in SASC’2007: Workshop Record of The State of the Art of Stream Ciphers, pp. 152–165, 2007.

[11] *K. Chen, M. Henricken, W. Millan, J. Fuller, L. Simpson, E. Dawson, H. Lee, and S. Moon,* “Dragon: A fast word based stream cipher,” in eSTREM, ECRYPT Stream Cipher Project, 2005. Report 2005/006.

[12] *M. Hell, T. Johansson, andW.Meier*, “Grain - a stream cipher for constrained environments,” citeseer.ist.psu.edu/732342.html.

[13] *C. D. Canniere and B. Preneel*, “TRIVIUMspecifications,” citeseer.ist.psu.edu/734144.html.

[14] *B. Gittins, H. A. Landman, S. O’Neil, and R. Kelson,* “A presentation on VEST hardware performance, chip area measurements, power consumption estimates and benchmarking in relation to the aes, sha-256 and sha-512.” Cryptology ePrint Archive, Report 2005/415, 2005. http://eprint.iacr.org/.

[15] *B. Preneel*, “A survey of recent developments in cryptographic algorithms for smart cards,” Comput. Networks, vol. 51, no. 9, pp. 2223–2233, 2007.

[16] *A. Canteaut*, “Open problems related to algebraic attacks on stream ciphers,” in WCC, pp. 120–134, 2005.

[17] E. *Dubrova,* A scalable method for constructing Galois NLFSRs with period 2^n-1 using cross-join pairs. IEEE Transactions on Information Theory. https://www.researchgate.net/profile/Elena_Dubrova/publication/267264884_A_ Scalable_Method_for_Constructing_Galois_NLFSRs_with_Period_2_n_-_1_using_Cross-Join_Pairs/links/5584137808ae89172b88a75d.pdf. 2013.

[18] *C. J. Jansen*, Investigations On Nonlinear Streamcipher Systems: Construction and Evaluation Methods. Ph.D. Thesis, Technical University of Delft, 1989.

[19] *D. Linardatos and N. Kalouptsidis*, “Synthesis of minimal cost nonlinear feedback shift registers,” Signal Process., vol. 82, no. 2, pp. 157–176. 2002.

[20] *J. S. I. Janicka-Lipska*, “Boolean feedback functions for full-length nonlinear shift registers,” Telecommunications and Informatioin Technology, vol. 5, pp. 28–29, 2004.

[21] *E. Dubrova*, A Method for Generating Full Cycles by a Composition of NLFSRs. Designs, Codes and Cryptography, ISSN 0925 – 1022, E – ISSN 1573 – 7586, November, Vol. 73, № 2, 469 – 486 p. 2014.

[22] *E. Dubrova,* A list of maximum – period NLFSRs. Cryptology ePrint Archive, Report 2012/166, 2012. http://eprint.iacr.org/2012/166. 2012.

[23] *E. Dubrova, M. Teslenko, H. Tenhunen*, On analysis and synthesis of (n,k) – non – linear feedback shift registers. in Design and Test in Europe, pp. 133–137. 2008.

[24] *T. Rachwalik, J. Szmidt, R. Wicik, J. Zabłocki,* Generation of Nonlinear Feedback Shift Registers with special – purpose hardware. Cryptology ePrint Archive: Report 2012/314, http://eprint.iacr.org/2012/314. 2012.

[25] *Потий А.В., Полуяненко Н.А*. Анализ свойств регистров сдвига с нелинейной обратной связью второго порядка генерирующих, последовательность с максимальным периодом // Прикладная радиоэлектроника. – 2008, № 3. – С. 282 – 290

[26] *Потій О.В., Полуяненко М.О*. Вибір утворюючих поліномів для регістра зсуву з нелінійним зворотним зв'язком другого порядку, що генерують послідовність з максимальним періодом. // COMPUTER SCIENCE AND CYBERSECURITY. – Харківський національний університет імені В.Н. Каразіна, Випуск 2(2), 2016. Електронний ресурс. Режим доступу: http://periodicals.karazin.ua/cscs/article/view/6209/5747

[27] Аналіз, розробка та дослідження постквантових криптографічних примітивів та обгрунтування умов їхнього застосування в Україні: звіт про НДР (проміжний). Том 1. – Аналіз та порівняльні дослідження симетричних криптографічних перетворень на постквантовий період / ХНУ ім. В.Н. Каразіна; кер. Кузнецов О.О.; вик.: Сватовський І.І.

Полуяненко Николай Александрович, аспирант кафедры безопасности информационных систем и технологий Харьковского национального университета им. В. Н. Каразина. Область научных интересов: криптографическая защита информации, поточные шифры, анализ функционирования и безопасности систем защиты информации.

УДК 004.056.55

Пошук регістрів зсуву з нелінійним зворотним зв'язком, що формує послідовність максимального періоду / М.О. Полуяненко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2016. – Том 15, №3. – С 245– 252.

У статті розглянуто один з важливих елементів генератора поточних шифрів – регістри зсуву з нелінійним зворотним зв'язком (РЗНЗЗ). Розглянуто проблему побудови РЗНЗЗ, що генерують послідовність максимального періоду (М-послідовність). Доповнюється раніше запропонований підхід до пошуку вказаних регістрів. Показано, що за допомогою запропонованого підходу можливо виключити більш ніж 99% РЗНЗЗ, які гарантовано не генерують М-послідовність, за допомогою чого значно зростає швидкість пошуку РЗНЗЗ, що генерують М-послідовність.

Ключові слова: регістри зсуву з нелінійним зворотним зв'язком, М-послідовність, нелінійні поліноми, поточні шифри, псевдо випадкові послідовності.

Табл.: 02. Іл.: 01. Біблогр.: 27 найм.

UDC 004.056.55

The searching of non-linear feedback shift registers forming a maximal length sequence / N.A. Poluyanenko // Applied Radio Electronics: Sci. Journ. – 2016. – Vol. 15, № 3. P. 245– 252.

In this paper one of the most important elements of a generator of stream ciphers – non-linear feedback shift registers (NLFSR) – is considered. The problem of constructing NLFSRs that generate a maximal length sequence (M-sequence) is considered. The previously proposed approach for searching such kind of registers is complemented. The approach, which can exclude 99% NLFSR that are not appropriate for the M-sequence, is shown. That approach greatly decreases time of searching NLFSRs that generate the M-sequence.

Keywords: non-linear feedback shift registers, M-sequence, non-linear polynoms, stream ciphers, pseudo-random sequences.

Tab.: 02. Fig.: 01. Ref.: 27 items.