

УДК 004.056.55

А.В. Потий¹, Н.А. Полуяненко²¹ Харківський національний університет імені В.Н. Каразіна, Харків² Харківський національний університет радіоелектроніки, Харків

К ВОПРОСУ О МАКСИМАЛЬНОМ ПЕРИОДЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГЕНЕРИРУЕМЫХ РЕГИСТРОВ СДВИГА С ЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ ВТОРОГО ПОРЯДКА

В статье проведено сравнение конструкций на основе регистров сдвига с нелинейной обратной связью второго порядка с регистрами сдвига с линейной обратной связью. Показано значительное преимущество в выборе РСНОС, генерирующих последовательность с максимальным периодом в сравнении с использованием РСЛОС. Получено выражение для определения результирующего периода последовательности, полученной путем суммирования нескольких последовательностей различных М-РСНОС. Даны рекомендации по выбору размерности образующих М-РСНОС для формирования суммарной последовательности максимального периода.

Ключевые слова: поточные шифры, нелинейные системы, период РСНОС.

Введение

При проектировании систем поточных шифров сформулировано ряд требований [1], которые включают в себя теоретические критерии Райнера Рюппеля [2]. В соответствии с этими требованиями схемы генераторов псевдослучайных последовательностей (ПСП) должны обладать:

- большим периодом выходной последовательности;
- хорошими статистическими свойствами выходной ПСП;
- нелинейностью, или, точнее говоря, высокой линейной сложностью выходной ПСП.

Хотя на сегодняшний момент не существует теоретического доказательства [3] необходимости и достаточности этих требований, но для создания криптографически стойких систем поточного шифрования они должны выполняться.

Основная часть существующих поточных схем шифрования состоит из отдельных блоков, основными из которых являются [1]:

- регистры сдвига с обратной связью (как правило, линейной);
- дискретные функции усложнения;
- запоминающие устройства;
- узлы, реализующие неравномерное движение.

Регистры сдвига с линейной обратной связью (РСЛОС) имеют ряд существенных недостатков связанных с их линейностью [4], но при этом обеспечивают большой период и хорошие статистические свойства ПСП, а остальные блоки используются для внесения нелинейности и усложнения в выходную последовательность.

С целью упрощения алгоритма генерации ПСП и при этом поддержания криптографической слож-

ности генерируемой последовательности на высоком уровне, предлагается вместо базового элемента на основе РСЛОС использовать регистры сдвига с нелинейной обратной связью (РСНОС), конструкция которого представлена на рис. 1.

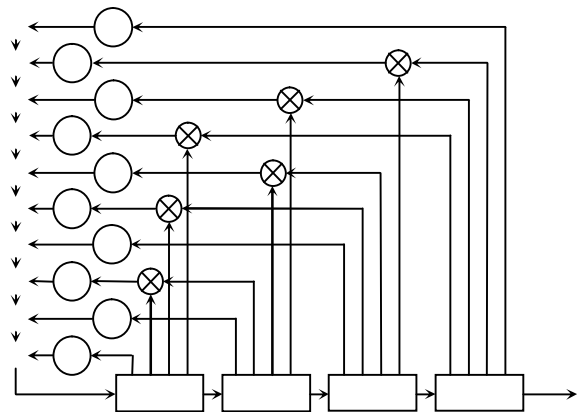


Рис. 1. Общий вид генератора ПСП, основанного на РСНОС при $L = 4$, где $a_{ij} \in \{0,1\}$ – блок умножения,

$q_i(t) \in \{0,1\}$ – значение i -го регистра в момент времени t , Q – генерируемая последовательность бит

В качестве обратной связи будем использовать побитовое сложение (обозначенное знаком \oplus) и нелинейную функцию – умножения (обозначенное знаком \otimes), через L обозначим количество регистров сдвига, используемых в системе. В нашей нелинейной функции обратной связи присутствуют слагаемые из произведений двух регистров, такую нелинейность назовем *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.

В результате применения РСНОС мы изначально закладываем нужную нам нелинейность в генерируемую последовательность, но при таком подходе возникает вопрос практически полной неизученности РСНОС в сравнении с РСЛОС. Одной из главных характеристик, как уже упоминалось выше, является изучение периода исследуемой системы, которая может состоять из одного или нескольких РСНОС.

Сравнение РСЛОС и РСНОС

Назовем последовательность, которая имеет максимальный период для заданного числа регистров L , M -последовательностью. РСНОС, генерирующие M -последовательность, назовем M -РСНОС.

Как показано в работе [5], максимально возможный период (T_{\max}) для заданного размера РСНОС - L , определяется как:

$$T_{\max} = 2^L - 1.$$

Символом n_L обозначим количество коэффициентов обратной связи a_{ij} для РСНОС второго по-

рядка, которое однозначно определяется для каждого L по формуле:

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

Как видим, максимально возможный период последовательности, который может генерировать РСНОС и РСЛОС совпадают. Множество различных комбинаций, которые можно создать на основе РСЛОС значительно меньше, чем множество аналогичных комбинаций на основе РСНОС и это множество будет определяться как $k = 2^{n_L}$. При этом число коэффициентов обратных связей для РСЛОС $n_L = L$.

Обозначим через M_0 полное множество регистров сдвига, которое генерирует M -последовательность. Для каждого L множество M_0 установлено экспериментальным путем.

Обобщенные результаты сравнения РСЛОС и РСНОС по вышеуказанным параметрам приведены в табл. 1. Следует учесть, что множество РСНОС включают в себя множество РСЛОС.

Таблица 1

Сравнение параметров РСЛОС и РСНОС

L	T_{\max}	РСЛОС			РСНОС		
		n_L	k	M_0	n_L	k	M_0
2	3	2	4	1	2	4	1
3	7	3	8	2	6	64	2
4	15	4	16	2	10	1 024	16
5	31	5	32	6	15	32 768	128
6	63	6	64	6	21	2 097 152	1 952
7	127	7	128	18	28	268 435 456	64 056
8	255	8	256	16	36	68 719 476 736	4 017 998
9	511	9	512	48	45	35 184 372 088 832	519 239 794

Как видно из табл. 1, у РСНОС имеется явное и значительное преимущества по сравнению с РСЛОС. Основным таким преимуществом является во много раз превосходящее количество различных M -РСНОС в сравнении с количеством M -РСЛОС для одинаковых значений L .

Период последовательности образованной в результате суммирования последовательностей от двух и более M -РСНОС

Широко известно, что для генерации последовательности заданной длины можно использовать сумму последовательностей от более коротких регистров сдвига. Однако, какие именно можно использовать при этом M -РСНОС и какой длины при этом будет суммарная последовательность, в доступной литературе не указывается.

Под суммой последовательностей РСНОС (обозначим её как Q^{sum}) будем понимать последователь-

ность, полученную в результате операции побитового суммирования (\oplus) двух и более последовательностей от РСНОС. Генерация последовательностей в каждом из РСНОС, участвующих в суммировании, производится независимо друг от друга.

Рассмотрим, какой суммарный период (T^{sum}) будет иметь последовательность, полученная в результате сложения двух и более последовательностей, сгенерированных M -РСНОС. Под T^{sum} понимаем наименьший получаемый период. Через T^1 обозначим период последовательности от первого M -РСНОС с длиной L^1 , T^2 период последовательности от второго M -РСНОС с длиной L^2 и т.д.

Суммарный период может быть выражен с помощью наименьшего общего кратного (НОК) или наибольшего общего делителя (НОД). В обобщенном виде можно записать наименьший период последовательности, который образуется в результате сложения нескольких последовательностей от M -РСНОС в следующем виде:

$$T^{\text{sum}} = \text{НОК}(T^1, T^2, T^3, \dots).$$

Как видно из полученных результатов $T^{\text{sum}} = T^1 \cdot T^2 \cdot T^3 \dots$ только в тех случаях, когда L^1, L^2 и т.д. являются взаимно простыми числами.

Следует отметить, что кратность периодов однозначно определяется кратностью L образующих полиномов.

Таким образом, результирующий период суммы двух РСНОС порождающих M -последовательностей можно записать в виде:

$$T^{\text{sum}} = \frac{(2^{L^1} - 1) \cdot (2^{L^2} - 1)}{2^{\text{НОД}(L^1, L^2)} - 1}.$$

В случае не соблюдения требования взаимно простых образующих L , возможны ситуации, когда даже при увеличении числа РСНОС, от которых проводится суммирование последовательностей, это не приводит к увеличению значения результирующего периода. В качестве примера можно привести суммирование последовательностей от РСНОС с $L = 4, 5, 6, 20$, при следующих их комбинациях:

$$Q(L = 6) \oplus Q(L = 20);$$

$$Q(L = 4) \oplus Q(L = 6) \oplus Q(L = 20);$$

$$Q(L = 5) \oplus Q(L = 6) \oplus Q(L = 20);$$

$$Q(L = 4) \oplus Q(L = 5) \oplus Q(L = 6) \oplus Q(L = 20).$$

В результате всех приведенных комбинаций период суммарной последовательности будет одинаков $T^{\text{sum}} = 22020075$.

Выводы

РСНОС имеют значительное преимущество в сравнении с РСЛОС в количестве возможных ком-

бинаций, которыми можно варьировать при создании необходимого регистра сдвига, а также в полном множестве регистров сдвига для заданного L , которые генерируют M -последовательность.

Период последовательности, образованной в результате суммирования последовательностей от различных M -РСНОС, равен произведению периодов исходных последовательностей, при условии взаимно простых значений L образующих M -РСНОС.

Получено соотношение для определения периода результирующей последовательности от суммирования последовательностей различных M -РСНОС, при условии не взаимно простых значений L .

Список литературы

1. Основные тенденции развития открытой криптографии (обзор по заказу sturgography.ru) // Опубликовано: geo.com.ru. [Электронный ресурс]. – Режим доступа к ресурсу: <http://images.geo.web.ru/pubd/2001/10/10/0001161293/tend.pdf>.
2. Rueppel R.A. *Analysis and Design of Stream Ciphers* / R.A. Rueppel. – Springer communications and control engineering series. – 1986. – 244 p.
3. Поточные шифры / А.В. Асосков, М.А. Иванов, А.А. Мирский, А.В. Рузин, А.В. Сланин, А.Н. Тютвин. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.
4. Schneier B. *A self-study course in block-cipher cryptanalysis* / B. Schneier // *Cryptologia*. – 2000. – Vol. XXIV, no. 1. – P. 18-33.
5. Потий А.В. Анализ свойств регистров сдвига с нелинейной обратной связью второго порядка генерирующих последовательность с максимальным периодом / А.В. Потий, Н.А. Полуяненко // *Прикладная радиоэлектроника*. – 2008. – № 3. – С. 282-290.

Поступила в редколлегию 1.06.2016

Рецензент: д-р техн. наук, проф. И.Д. Горбенко, Харьковский национальный университет имени В.Н. Каразина, Харьков.

ДО ПИТАННЯ ПРО МАКСИМАЛЬНИЙ ПЕРІОД ПОСЛІДОВНОСТЕЙ РЕГІСТРІВ ЗРУШЕННЯ, ЩО ГЕНЕРУЮТЬСЯ, З ЛІНІЙНИМ ЗВОРОТНИМ ЗВ'ЯЗКОМ ДРУГОГО ПОРЯДКУ

О.В. Потій, М.О. Полуяненко

У статті проведено порівняння конструкцій на основі регістрів зсуву з нелінійним зворотним зв'язком другого порядку з регістрами зсуву з лінійним зворотним зв'язком. Показано значну перевагу у виборі РЗНОЗ, що генерують послідовність максимального періоду в порівнянні з використанням РЗЛОЗ. Отримано вираз для визначення результуючого періоду послідовності, отриманої шляхом підсумовування декількох послідовностей різних M -РЗНОЗ. Дана рекомендація щодо вибору розмірності утворюючих M -РЗНОЗ для формування сумарної послідовності з максимальним періодом.

Keywords: stream ciphers, nonlinear systems, period of SRNLF.

THE MAXIMUM PERIOD OF THE SEQUENCES GENERATED BY SRNLF OF THE SECOND ORDER

O.V. Potii, N.A. Poluyanenko

The comparing of constructions based on shift registers with a nonlinear feedback of the second order with shift registers with a linear feedback is considered. It is shown that there is a significant advantage in choosing SRNLF generating the sequence with a maximal period in comparing with using SRLF. The expression for determination of the sequence resulting period got by means of summation of a few sequences of different M -SRNLF is received. The recommendations in choosing a dimensionality of forming M -SRNLF to form the summary sequence of a maximal period are given.

Keywords: stream ciphers, nonlinear systems, period of SRNLF.