УДК 004.056.5

А.А. КУЗНЕЦОВ, д-р техн. наук, А.В. ПОТИЙ, д-р техн. наук,
Н.А. ПОЛУЯНЕНКО, канд. техн. наук, И.В. СТЕЛЬНИК

НЕЛИНЕЙНЫЕ ФУНКЦИИ УСЛОЖНЕНИЯ ДЛЯ ПОТОКОВЫХ СИММЕТРИЧНЫХ ШИФРОВ

Введение

Анализ современных схем потокового шифрования, таких как SNOW 2.0 0, Decim 0 KCipher-2 0, Sosemanuk 0, Grain 0, MICKEY 2.0 0, Trivium 0 показывает, что основными компонентами являются итеративные генераторы битового потока и функция усложнения, формирующая из некоторых комбинаций битов внутреннего состояния выходной блок.

Итеративные генераторы битового потока, как правило, строятся на основе регистров сдвига с линейными обратными связями (РСЛОС), основная задача которых гарантировать неповторимость внутреннего состояния генератора достаточно большой промежуток времени его работы и гарантировать, что обеспечены хорошие локальные статистические свойства. Данным требованиям отвечают регистры, формирующие последовательность де Брейна. Однако данную последовательность можно генерировать также и регистрами сдвига с нелинейными обратными связями (РСНОС). Применение в качестве итеративных генераторов РСНОС позволяют сохранить все достоинства использования РСЛОС, но при этом генераторы лишены главного недостатка РСЛОС – линейности.

Вместе с тем, при проектировании криптографических систем с применением РСНОС появляются новые проблемные вопросы, связанные с выбором нелинейного регистра. Теория РСЛОС достаточно хорошо изучена 0, РСНОС изучены намного меньше, чем РСЛОС 0. Первый алгоритм для построения наименьшего РСНОС заданной, двоичной последовательностью был представлен Янсеном (Jansen) в 1991 году 0, 0. Альтернативные алгоритмы были даны 0].

Известно, как построить РСЛОС с максимальным периодом, их функции обратной связи соответствуют примитивному многочлену над F_2. В общем случае неизвестно, как построить все РСНОС с максимальным периодом. Основной метод заключается в поиске таких регистров с соответствующими свойствами. Как правило, все приведенные в литературе регистры с нелинейной обратной связью имеют достаточно сложную структуру и состоят не из одного структурного элемента. Если же РСНОС имеет простую структуру, то он является регистром малого размера.

Отсутствуют какие-либо общие методы проектирования РСНОС максимального периода [8, 15]. Построение специального класса РСНОС с максимальным периодом было дано Миккелвайтом (Mykkeltveit) и др. [16]. В работе Е. Дубровой (E. Dubrova) [15] приведен пример сдвига регистра Галуа размером $L = 100$ ячеек, который генерирует последовательность с максимальным периодом, но эта последовательность не обладает свойством последовательности де Брейна, то есть некоторые кортежи битов появляются более одного раза в последовательности.

При этом с увеличением размера используемого регистра, возрастает его конструктивная сложность. Если удается сформировать РСНОС формирующий последовательность де Брейна необходимого размера, то его структура будет настолько сложной, что его реализация в системах шифрования, в качестве итеративного генератора, будет недопустимо ресурсоемкой.

Сложность конструкции напрямую связана с размерами и стоимостью аппаратной реализации шифра, который ее использует, а также в большинстве случаев влияет на его быстродействие. Чем меньше конструктивная сложность функции, тем проще ее схемная реализация. Особенно это актуально для так называемой легковесной (или малоресурсной) криптографии.

С другой стороны, если изначально производить поиск РСНОС с заданными конструктивными особенностями, в частности – простота реализации, то найденный регистр может иметь уязвимости к определенным типам атак, для нейтрализации которых необходимо вводить в алгоритм дополнительные узлы и, как следствие, увеличивать общую ресурсоемкость всей схемы.

Возникает вопрос о возможности оптимизации структуры РСНОС между простотой аппаратной/программной реализации и соответствием некоторым заданным свойствам формируемой последовательности. Под простотой реализации будем понимать число операций, необходимое и достаточное для вычисления следующего состояния итеративного генератора.

Приведенные в работе результаты отражают взаимосвязь конструктивных характеристик РСНОС (таких как максимальная алгебраическая степень, количество мономов) и некоторых необходимых криптографических свойств формируемой им последовательности (автокорреляции и линейной сложности).

1. Полученные результаты

1.1. Булевы функции

Для дальнейшего изложения приведем некоторые определения, которыми будем пользоваться в работе:

F_2 – конечное поле из двух элементов, 0 и 1. Операции в F_2 – умножение и сложение по модулю 2;

V_L L – мерное векторное пространство над полем F_2, $V_L = (F_2)^L$. Сложение в пространстве V_L побитовое по модулю 2.

Булева функция от L переменных есть отображение из V_L в F_2. Расширенные булевы функции – отображения из V_L в Z (множество целых чисел). Еще более общие псевдобулевы функции – отображения из V_L в R (множество действительных чисел).

Число векторов пространства V_L равно 2^L как число всевозможных комбинаций L базисных векторов с коэффициентами 0 и 1.

Пусть $Z_2 = \{0,1\}$. Через $Z_2^{\,L}$ будем обозначать множество всех двоичных векторов $x = (x_1, \ldots, x_L)$ длины L. Будем считать, что все векторы лексикографически упорядочены.

Произвольная функция отображения из множества $Z_2^{\,L}$ в множество Z_2 называется *булевой функцией от L переменных*.

Каждую булеву функцию от L переменных можно однозначно определить вектором ее значений длины 2^L. Например, функциям f и g соответствуют векторы (1001) и (00010110). Пусть далее f обозначает вектор значений длины 2^L функции f. Будем считать, что аргументы функции (т.е. векторы длины L) перебираются в лексикографическом порядке.

Пусть $\oplus$ обозначает сложение по модулю 2 (операцию XOR). Известно, что каждая булева функция однозначно может быть задана своей *алгебраической нормальной формой* (АНФ), в отечественной литературе АНФ также называют полиномом Жегалкина.

АНФ есть выражение булевой функции в виде

$$f(x_1, \ldots x_L) = \bigoplus_{N \in P\{1,2,\ldots,L\}} a_N \prod_{i \in N} x_i \ , \qquad (1)$$

где $P\{1,2,\ldots L\}$ – множество всех подмножеств $\{1,2,\ldots L\}$ (булеан), $a_N \in F_2$.

Для вычисления АНФ заданной функции имеются несложные алгоритмы (см., например, 0).

Степень монома (булевый одночлен) $x^N = \prod_{i \in N} x_i$ определяется как $|N|$ (число элементов подмножества N).

Алгебраической степенью $\deg(f)$ или *порядком нелинейности* булевой функции f называется число переменных в самом длинном слагаемом (мономе) ее АНФ. Булева функция степени 1 называется *аффинной*. Ее АНФ имеет вид $f(x) = a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_L x_L \oplus b =$

$= \langle a, x \rangle \oplus b$, где $b \in F_2, a \in V_L$. Функция называется квадратичной, кубической и т.д., если ее алгебраическая степень равна соответственно 2, 3 и т.д.

1.2. Последовательность де Брейна

Пусть $A = a_1, a_2, \ldots, a_{2^L-1}, a_{2^L}$ последовательность длины 2^L из элементов алфавита $\{0,1\}$.

A называется *последовательностью де Брейна* порядка L, если среди всех кортежей длины L: $L\,(a_1, a_2, \ldots, a_L)$, $(a_2, a_3, \ldots, a_{L+1})$, …, $(a_{2^L-L+1}, a_{2^L-L+2}, \ldots, a_{2^L})$, каждый из возможных кортежей присутствует и встречается ровно один раз, т.е. встречаются всевозможные 2^L комбинации над алфавитом $\{0,1\}$ 0.

Аналогичные последовательности длины $2^L - 1$ без кортежа из одних нулей называются *модифицированными последовательностями де Брейна*.

Легко заметить, что из последовательности де Брейна можно получить модифицированную последовательность де Брейна вычеркиванием одного нуля, а из модифицированной последовательности де Брейна – последовательность де Брейна добавлением одного нуля.

Аналогичные последовательности можно построить для алфавита из k элементов. Например, 0011 и 002212011 являются последовательностями де Брейна порядка $L = 2$ над алфавитами $\{0,1\}$ и $\{0,1,2\}$ соответственно. Последовательности де Брейна используются в криптографии в силу своих хороших статистических свойств – не отличимых, в статистическом смысле, от истинно случайных последовательностей.

В 1894 г. С. Флай Санте Марие 0 и в 1946 г. де Брейн 0 доказали существование таких последовательностей для любого натурального числа L, над любым алфавитом из k-элементов и показали, что число различных последовательностей (B_n)

$$B_n = \left[(k-1)!\right]^{k^{L-1}} k^{k^{L-1}-L} \tag{2}$$

(две последовательности считаются различными, если любую из них невозможно получить циклическим сдвигом другой). Для случая булевых функций, т.е. $k = 2$, выражение (2) примет вид

$$B_n = 2^{2^{L-1}-L} \tag{3}$$

Для оценки полученных результатов в табл. 1 приведены количественные значения числа различных последовательностей де Брейна полученных в соответствии с выражением (2).

$$B_n = \left[(k-1)!\right]^{k^{L-1}} k^{k^{L-1}-L}.$$

Как видим, уже при $L = 7$ и $k = 2$ количество различных последовательностей де Брейна приобретает размер затрудняющий обработку (поиск, хранение, анализ) всего множества.

Добавим, что число примитивных полиномов степени L равно

$$\frac{\varphi\left(2^L - 1\right)}{L}, \tag{4}$$

где φ – функция Эйлера.

Таблица 1

Число различных последовательностей де Брейна при заданных L и k

L	k		
	2	3	4
2	1	24	20 736
3	2	373 248	$\approx 1.8 \cdot 10^{20}$
4	16	$\approx 1.2 \cdot 10^{19}$	$\approx 8.4 \cdot 10^{85}$
5	2 048	$\approx 4.4 \cdot 10^{60}$	$\approx 2.1 \cdot 10^{350}$
6	67 108 864	$\approx 1.7 \cdot 10^{186}$	$\approx 5.3 \cdot 10^{1409}$
7	2^{57}	$\approx 1 \cdot 10^{1698}$	$\approx 1.4 \cdot 10^{5649}$
8	2^{120}	$\approx 1 \cdot 10^{1698}$	$6^{16384} \cdot 4^{16376}$
9	2^{247}	$\approx 1.4 \cdot 10^{5101}$	$6^{65536} \cdot 4^{65527}$

Обзор 0 дает наиболее полный экскурс в теорию последовательностей де Брейна и историю их использования для решения различных задач.

М-РСНОС будем называть те РСНОС, которые реализуют булевы функции, формирующие модифицированные последовательности де Брейна. Если же эти функции являются линейными – то соответствующие регистры будем назвать М-РСЛОС. В общем случае М-РСЛОС являются частным случаем М-РСНОС.

Период последовательности де Брейна $(T_{ПБ})$ определяется размером алфавита или, как его еще называют, основанием последовательности де Брейна k, а также разрядностью состояний (числом ячеек памяти итеративного генератора) – L:

$$T_{ПБ} = k^L. \tag{5}$$

И, соответственно, период модифицированной последовательности де Брейна (T) будет определен как

$$T = k^L - 1. \tag{6}$$

1.3. Максимальная алгебраическая степень АНФ последовательностей де Брейна

Максимальная алгебраическая степень АНФ для М-РСНОС при $k = 2$ определяется как

$$\deg(f) \le L - 2 \text{ (для } L > 2). \tag{7}$$

Данное утверждение было описано еще Голомбом в работе 0.

Нами были получено распределение числа модифицированных последовательностей де Брейна в зависимости от порядка нелинейности формирующего данную последовательность М-РСНОС или, что равносильно, от максимальной алгебраической степени АНФ формирующего полинома. Полученное распределение для $k = 2$ приведено в табл. 2.

Таблица 2

Распределения числа М-РСНОС в зависимости от порядка нелинейности $\deg(f)$ для $k = 2$.

	Количество М-РСЛОС	Количество М-РСНОС 2-го порядка	Количество М-РСНОС 3-го порядка	Количество М-РСНОС 4-го порядка
2	1	–	–	–
3	2	–	–	–
4	2	14	–	–
5	6	122	1 920	–
6	6	1 946	2 095 200	65 011 712
7	18	64 038	*неизвестно*	*неизвестно*
8	16	4 017 982	*неизвестно*	*неизвестно*
9	48	519 239 746	*неизвестно*	*неизвестно*

Отметим, что с увеличением алгебраической степени АНФ экспоненциально увеличивается число полиномов, формирующих модифицированные последовательности де Брейна, а следовательно, и вероятность того, что произвольным образом выбранный М-РСНОС будет иметь более алгебраическую степень.

1.4 Количество мономов АНФ М-РСНОС

Пусть τ – число мономов в рекуррентном соотношении определяющая обратную связь в РСНОС. Для всех М-РСНОС τ – четное число. Распределение общего количества мономов в зависимости от τ для $4 \le L \le 6$ опубликовано в 0. Также в 0 доказано, что минимальное количество мономов в полиноме соответствует 2 (достигается только для М-РСЛОС), а максимальное вычисляется соотношением $2^{L-1}-2$ (кроме $L=2$). Распределение имеет гауссовский характер.

Нами получено и приведено в табл. 3 аналогичное распределение, учитывающее $\deg(f)$.

Таблица 3

Распределение количества мономов АНФ М-РСНОС
в зависимости от порядка нелинейности для $k=2$

τ	Количество о М-РСЛОС	Количество М-РСНОС 2-го порядка	Количество о М-РСНОС 3-го порядка	Количество М-РСНОС 4-го порядка
$L=2$				
1	1	–	–	–
$L=3$				
2	2	–	–	–
$L=4$				
2	2	–	–	–
4	–	10	–	–
6	–	4	–	–
$L=5$				
2	2	–	–	–
4	4	26	66	–
6	–	66	426	–
8	–	26	858	–
10	–	4	490	–
12	–	–	76	–
14	–	–	4	–
$L=6$				
2	2	–	–	–
4	4	42	94	106
6	–	312	4 414	6 512
8	–	782	50 380	147 042
10	–	596	239 916	1 322 050
12	–	192	553 804	5 890 004
14	–	22	658 398	14 115 280
16	–	–	420 692	19 139 124
18	–	–	141 894	15 146 272
20	–	–	23 808	7 057 286
22	–	–	1 742	1 892 112
24	–	–	58	274 994
26	–	–	–	20 294
28	–	–	–	628
30	–	–	–	8

Исходя из принципов комбинаторики можно показать, что количество возможных обратных связей для РСНОС размерностью в L ячеек и порядком нелинейности $\deg(f)$ определяется соотношением

$$n_L^{\deg(f)} = L \cdot \left(1 + \sum_{i=1}^{\deg(f)-1} \frac{\prod_{j=1}^{i} (L-j)}{(1+i)!} \right). \quad (8)$$

Как видим из табл. 4, количество мономов для изученных М-РСНОС лежит в диапазоне $2 \le \tau \le \frac{2}{3} n_L^{\deg(f)}$, а пик распределения приблизительно соответствует $\frac{1}{3} n_L^{\deg(f)}$.

1.5. Автокорреляционная функция

Пусть $S = (s(1), s(1), s(3), \ldots)$– периодическая последовательность с периодом T. *Автокорреляционная функция* (АКФ) S является целочисленной функцией:

$$AC(t) = \frac{1}{T} \sum_{t=1}^{T} (2s(i)-1)(2s(i+t)-1), \quad (9)$$

для $0 \le t \le T-1$

Для примера на рис. 1 показана АКФ М-РСЛОС при $L=4$ и $T=15$, определяемая рекуррентным соотношением $s_{(5+t)} = s_{(4+t)} + s_{(1+t)}$, а на рис. 2 – АКФ М-РСНОС при $L=4$, определяемая рекуррентным соотношением $s_{(5+t)} = s_{(4+t)} + s_{(3+t)} + s_{(2+t)} +$

$+ s_{(1+t)} + s_{(4+t)} \cdot s_{(2+t)} + s_{(3+t)} \cdot s_{(2+t)}$.

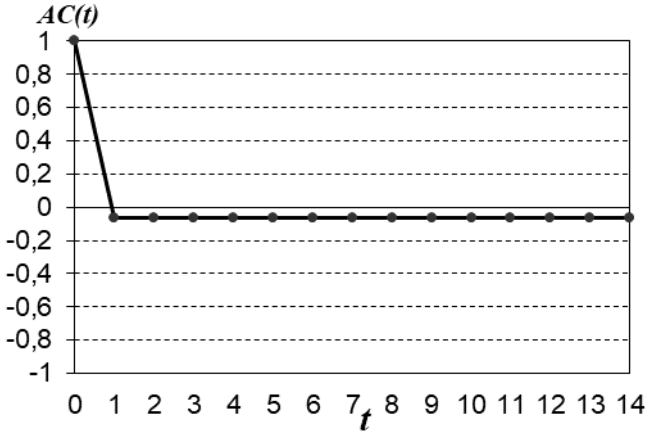

Рис. 1. АКФ для М-РСЛОС при $L=4$

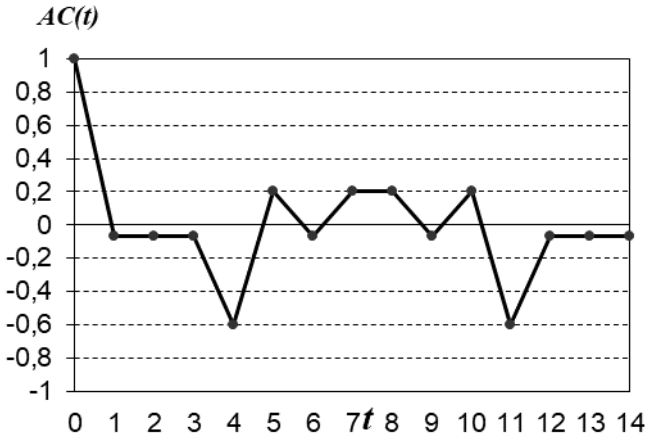

Рис. 2. АКФ для М-РСНОС при $L=4$

Анализируя полученные результаты, можно утверждать, что все АКФ имеют симметричный вид относительно середины графика (не включая нулевое значение, соответствующее отсутствию сдвижки); только М-РСЛОС имеют постоянную и минимальную корреляцию со своими сдвинутыми копиями последовательности.

Кроме того, значение АКФ значительно меняется в зависимости от выбранного М-РСНОС при формировании результирующей последовательности. С практической точки зрения понятно, что чем меньше коррелирует последовательность со своей же сдвинутой копией, тем менее она подвержена атакам, использующим данную уязвимость. Причем важно, чтобы не было корреляции при любой сдвижке.

Введем значение АКФ, которое будет характеризовать ее максимальное значение (взятое по модулю) для всех $1 \le t \le T-1$, обозначим как $AC_{\max}$. Значение $AC_{\max}$ ограничено снизу выражением $AC_{\max} \ge 1/T$, достигаемое только при использовании в качестве функций обратных связей М-РСЛОС.

Обобщенные результаты для значения $AC_{\max}$ приведены в табл. 4 – 7.

Таблица 4

Распределение максимального значения АКФ для $L = 3 (T = 7)$

$AC_{\max}$	Количество М-РСНОС	Количество М-РСЛОС
$1/T = 0.14286$	**2**	2

Таблица 5

Распределение максимального значения АКФ для $L = 4 (T = 15)$

$AC_{\max}$	Кол-во М-РСНОС	Кол-во М-РСЛОС	Кол-во М-РСНОС 2-го порядка
$1/T = 0.06667$	**2**	2	–
$5/T = 0.33333$	**10**	–	10
$9/T = 0.60000$	**4**	–	4

Таблица 6

Распределение максимального значения АКФ для $L = 5 (T = 31)$

$AC_{\max}$	Кол-во М-РСНОС	Кол-во М-РСНОС 2-го порядка	Кол-во М-РСНОС 3-го порядка
$1/T = 0.03226$	**6**	–	–
$5/T = 0.16129$		–	56
$7/T = 0.22581$	**154**	8	146
$9/T = 0.29032$	**1156**	78	1078
$11/T = 0.35484$	**170**	12	158
$13/T = 0.41935$	**382**	14	368
$15/T = 0.48387$	**8**	–	8
$17/T = 0.54839$	**110**	10	100
$21/T = 0.67742$	**6**	–	6

Таблица 7

Распределение максимального значения АКФ для $L = 6 (T = 63)$

$AC_{\max}$	Кол-во М-РСНОС 2-го порядка	Кол-во М-РСНОС 3-го порядка	Кол-во М-РСНОС 4-го порядка
$5/T = 0.07937$	–	–	12
$7/T = 0.11111$	–	10	468
$9/T = 0.14286$	10	12 772	391 484
$11/T = 0.17460$	44	49 556	1 534 900
$13/T = 0.20635$	212	351 690	10 906 882
$15/T = 0.23810$	222	274 756	8 522 742
$17/T = 0.26984$	920	766 838	23 851 328
$19/T = 0.30159$	128	167 810	5 202 124
$21/T = 0.33333$	242	269 832	8 344 838
$23/T = 0.36508$	32	30 922	955 434
$25/T = 0.39683$	70	143 930	4 450 510
$27/T = 0.42857$	4	3 336	100 228
$29/T = 0.46032$	12	10 684	346 834
$31/T = 0.49206$	–	174	5 480
$33/T = 0.52381$	50	12 216	377 528
$35/T = 0.55556$	–	8	116
$37/T = 0.58730$	–	140	4 656
$41/T = 0.65079$	–	526	16 146
$45/T = 0.71429$	–	–	2

Как видим, изученные последовательности, сформированные нелинейными регистрами, уступают по характеристикам АКФ последовательностям, сформированным линейными регистрами. Лучшее значение для изученных М-РСНОС соответствует $AC_{\max} = 5/T$ и достигается при наличии максимального порядка нелинейности.

Характер распределения примерно одинаков для любого порядка нелинейности.

1.6. Линейная сложность

Линейная сложность (Li) псевдослучайной последовательности – самый короткий регистр сдвига, с помощью которого формируется данная периодическая последовательность, при условии, что первые Li значений последовательности являются начальными заполнениями регистра.

Оценка линейной сложности является одним из основных параметров системы. Любая последовательность, которую можно сгенерировать автоматом (линейным или нелинейным) над конечным полем, имеет конечную линейную сложность. Таким образом, можно построить алгоритм, с помощью которого определяется линейная сложность любой последовательности, независимо от способа ее генерации, при этом знание структуры схемы, формирующей исходную последовательность, является лишним.

Для вычисления линейной сложности наиболее распространенным является алгоритм Берлекэмпа – Месси, суть которого изложена в 0, 0.Таким образом, большая линейная сложность формируемой последовательности является необходимым (но недостаточным) условием практической стойкости генераторов псевдослучайных последовательностей.

В идеале линейная сложность должна быть близкой или равной периоду последовательности. Линейная сложность была получена еще Golomb в работе 0.

М-РСНОС имеют в большинстве случаев максимальную линейную сложность $Li_{\max} = 2^L - 2$ или близкую к ней. Нами получены и приведены результаты распределения линейной сложности с учетом порядка нелинейности.

В табл. 8 – 10 приведено распределение линейной сложности для всего множества полиномов, формирующих последовательность де Брейна размерностью $L = 2,\ldots,6$, а также дано распределение в зависимости от порядка нелинейности формирующего последовательность регистра. В табл. 11 – 13 приведено распределение линейной сложности для М-РСЛОС и М-РСНОС 2-го порядка при $7 \le L \le 9$.

Таблица 8

Распределение линейной сложности последовательностей де Брейна для $L = 4$

Li	Кол-во М-РСНОС	Кол-во М-РСЛОС	Кол-во М-РСНОС 2-го порядка
4	**2**	6	–
12	**4**	–	4
14	**10**	–	10

Таблица 9

Распределение линейной сложности последовательностей де Брейна для $L = 5$

Li	Кол-во М-РСНОС	Кол-во М-РСЛОС	Кол-во М-РСНОС 2-го порядка	Кол-во М-РСНОС 3-го порядка
5	**6**	6	–	–
15	**10**	–	–	10
20	**4**	–	–	4
25	**306**	–	20	286
30	**1 722**		102	1620

Таблица 10

Распределение линейной сложности последовательностей де Брейна для $L = 6$

Li	Кол-во М-РСНОС	Кол-во М-РСНОС 2-го порядка	Кол-во М-РСНОС 3-го порядка	Кол-во М-РСНОС 4-го порядка
6	**6**	–	–	–
27	**10**	–	–	10
30	**8**	–	–	8
32	**12**	–	–	12
33	**8**	–	–	8
35	**62**	–	–	62
36	**152**	–	10	142
38	**478**	–	14	464
39	**1 036**	–	48	988
41	**3 572**	–	106	3 466
42	**6 100**	–	200	5 900
44	**17 240**	–	536	16 704
45	**28 702**	4	936	27 762
47	**86 056**	–	2 650	83 406
48	**134 290**	4	4 184	130 102
50	**401 102**	8	12 692	388 402

51	**453 734**	20	14 184	439 530
53	**1 364 978**	48	43 184	1 321 746
54	**1 819 148**	68	56 930	1 762 150
56	**5 453 680**	158	171 298	5 282 224
57	**3 190 982**	126	100 724	3 090 132
59	**9 557 084**	256	297 988	9 258 840
60	**11 148 860**	338	347 518	10 801 004
62	**33 441 564**	916	1 041 998	32 398 650

Таблица 11

Распределение линейной сложности последовательностей де Брейна для М-РСНОС с $\deg(f) \le 2$ при $L = 7$

Li	Количество М-РСЛОС	Количество М-РСНОС 2-го порядка
7	18	–
105	–	22
112	–	594
119	–	8 044
126	–	55 378

Таблица 12

Распределение линейной сложности последовательностей де Брейна для М-РСНОС с $\deg(f \le 2)$ при $L = 8$

Li	Количество М-РСЛОС	Количество М-РСНОС 2-го порядка
8	16	–
208	–	2
214	–	2
218	–	2
220	–	6
222	–	18
224	–	26
226	–	96
228	–	204
230	–	726
232	–	1 020
234	–	2 914
236	–	5 954
238	–	18 168
240	–	17 578
242	–	52 538
244	–	96 554
246	–	289 222
248	–	147 584
250	–	440 762
252	–	738 236
254	–	2 206 370

Таблица 13

Распределение линейной сложности последовательностей де Брейна для М-РСНОС с $\deg(f) \le 2$ при $L = 9$

Li	Количество М-РСЛОС	Количество М-РСНОС 2-го порядка
9	48	
456	–	2
459	–	2
462	–	6
465	–	34
468	–	30
471	–	504
474	–	1 866
477	–	1 386
480	–	21 112
483	–	74 458
486	–	42 542
489	–	599 644
492	–	2 097 832
495	–	795 706
498	–	11 163 082
501	–	39 051 092
504	–	7 268 192
507	–	101 824 464
510	–	356 297 792

Как видим из полученных результатов, подавляющая часть М-РСНОС имеет максимальную или отличающуюся на несколько единиц от максимальной линейной сложности. Характер распределения сохраняется для любого значения $\deg(f)$.

Профиль линейной сложности изученных последовательностей близок к математическому ожиданию линейной сложности, как и для истинно случайной последовательности.

Выводы

Булевы функции, формирующие последовательность де Брейна, привлекательны в качестве итеративных генераторов в потоковых шифрах в силу своих хороших локальных статистических характеристик, максимального периода формируемой последовательности и простоты реализации.

Использование нелинейности в булевых функциях влечет увеличение конструктивных характеристик.

Так, большинство М-РСНОС имеет в своей структуре количество мономов равное 1/3 от максимального значения. К примеру, для $L = 32$ большинство М-РСНОС будет иметь порядка 10^9 слагаемых, а каждое слагаемое будет содержать произведение до 30 различных значений, что, с точки зрения практической реализации, для систем потокового шифрования неприемлемо. Однако, как показано в работе, имеются М-РСНОС с минимальным количеством коэффициентов обратной связи.

Изученные последовательности, сформированные нелинейными регистрами, уступают по характеристикам АКФ последовательностям, сформированными линейными регистрами.

Лучшее значение для изученных М-РСНОС соответствует $AC_{\max} = 5/T$ (для М-РСЛОС все $AC_{\max} = 1/T$) и достигается при наличии максимального порядка нелинейности. Характер распределения примерно одинаков для любого порядка нелинейности. Однако, учитывая относительно равномерное распределение $AC_{\max}$, можно предположить, что произвольно

взятая булева функция, формирующая последовательность де Брейна, будет иметь невысокий показатель $AC_{\max}$.

В отличие от М-РСЛОС подавляющая часть М-РСНОС с $\deg(f) \geq 2$ имеет максимальную или отличающуюся на несколько единиц от максимальной линейную сложность $Li_{\max} = 2^L - 2$. Характер распределения сохраняется для любого значения $\deg(f) \leq 2$. При этом профиль линейной сложности близок к математически ожидаемому, как и для истинно случайных последовательностей.

Таким образом, поиск конструктивно простых РСНОС, формирующих последовательность де Брейна, а также оптимизация структуры для соответствия необходимым криптографическим свойствам, является сложной задачей, требующей дальнейшего изучения.

Список литературы:

1. Marcus Schafheutle. A First Report on the Stream Cipher SNOW. http://www.cryptonessie.org

2. C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert. Decim – A new Stream Cipher for Hardware applications. In ECRYPT Stream Cipher Project Report 2005/004. Available at http://www.ecrypt.eu.org/stream/

3. S. Kiyomoto, T. Tanaka, and K. Sakurai, "A word-oriented stream cipher using clock control," Workshop Recod of SASC 2007, pp.260–274, January 2007 [Електронний ресурс]. – Режим доступу: https://www.cosic.esat.kuleuven.be/ecrypt/stream/papersdir/2007/029.pdf

4. The eSTREAM Project – eSTREAM Phase 3. SOSEMANUK (Portfolio Profile 1). [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org/ stream /sosemanukpf.html

5. The eSTREAM Project – eSTREAM Phase 3. Grain (Portfolio Profile 2). [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org/stream/ grainpf.html

6. The eSTREAM Project – eSTREAM Phase 3. MICKEY (Portfolio Profile 2). [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org/stream/ mickeypf.html

7. The eSTREAM Project – eSTREAM Phase 3. Trivium (Portfolio Profile 2). [Електронний ресурс]. – Режим доступу: http://www.ecrypt.eu.org/stream/triviumpf.html

8. Dabrowski P., Łabuzek G., Rachwalik T., Szmidt J. Searching for Nonlinear Feedback Shift Registers with Parallel Computing. [Електронний ресурс]. 2013 URL: https://eprint.iacr.org/2013/542.pdf (дата звернення: 07.10.2016).

9. Fredricksen H. A survey of full length nonlinear shift register cycle algorithms," SIAM Review. 1982, vol. 24, № 2. P. 195–221.

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

11. Jansen C.J. The maximum order complexity of sequence ensembles. Lecture Notes in Computer Science, Adv. Cryptology-Eupocrypt'1991, Berlin, Germany. 1991, vol. 547, P. 153–159.

12. Linardatos D., Kalouptsidis N. Synthesis of minimal cost nonlinear feedback shift registers // Signal Process. – 2002. – Vol. 82, № 2. – P. 157–176.

13. Rizomiliotis P., Kalouptsidis N. Results on the nonlinear span of binary sequences // IEEE Transactions on Information Theory. – 2005. – Vol. 51, № 4. – P. 1555–5634.

14. Limniotis K., Kolokotronis N., Kalouptsidis N. On the nonlinear complexity and Lempel-Ziv complexity of finite length sequences // IEEE Transactions on Information Theory. – 2007. – vol. 53, № 11. – P. 4293–4302.

15. E. Dubrova, A scalable method for constructing Galois NLFSRs with period 2n-1 using cross-join pairs // IEEE Transactions on Information Theory. – 2013. – vol. 59(1). – P. 703-709.

16. Mykkeltveit J., Siu M-K., Tong P. On the cyclic structure of some nonlinear shift register sequences // Inform. and Control. – 1979. – vol. 43. – P. 202-215.

17. Carlet C. Boolean functions for cryptography and error correcting codes // In: Crama Y., Hammer P. L. (Eds.), Boolean Methods and Models, Cambridge University Press, http://www-rocq.inria.fr/secret/Claude.Carlet/ chap-fcts-Bool.pdf

18. Knuth, D. The Art of Computer Programming. Vol. II. Seminumerical Algorithms. – USA, Commonwealth of Massachusetts: Addison-Wesley, 1969. – P.634.

19. Flye-Sainte Marie C. Solution to question number 48 // l'Intermediaire des Mathematiciens. –1894. – V. 1. – P. 107-110.

20. de Bruijn N.G. A combitorial problem // Nederl. Akad. Wetensch. Proc. –1946. – V. 49. – P. 758-764.

21. H. Fredricksen. A survey of full length nonlinear shift register cycle algorithm // SIAM Review, 24(2):195–221, 1982.

22. Mayhew G.L., Golomb S.W. Characterizations of generators for modified de Bruijn sequences. Advances in applied mathematics 13(4), 454-461 (1992) https://www.sciencedirect.com/ science/article/pii/019688589290021N

23. Berlekamp E. R. Algebraic Coding Theory. McGraw-Hill, NY, 1968. – P.474.

24. McWilliams F.J. Sloane N.J. The Theory of Error-Correcting Codes // North-Holland, 1978. – P. 762.

25. Mayhew G.L., Golomb S.W. Linear spans of modified de Bruijn sequences // IEEE Trans. Inform. Theory. – 1990. – № 36(5). – P. 1166–1167.

Харьковский национальный
университет имени В.Н. Каразина;
АО «Институт информационных технологий», Харьков;
Государственная служба специальной связи и защиты
информации Украины, Киев

Поступила в редколлегию 22.10.2018