УДК 004.056.5

А.А. КУЗНЕЦОВ, д-р техн. наук, А.В. ПОТИЙ, д-р техн. наук,
Н.А. ПОЛУЯНЕНКО, канд. техн. наук, С.Г. ВДОВЕНКО

КОМБИНИРУЮЩИЕ И ФИЛЬТРУЮЩИЕ ФУНКЦИИ НА ОСНОВЕ РЕГИСТРОВ СДВИГА С НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ

1. Введение

1.1. Исследуемая модель

Рассмотрим общую структурную схему комбинирующего генератора (рис. 1) и фильтрующего генератора (рис. 2) псевдослучайной последовательности (ПСП) с применением нескольких регистров сдвига с линейными обратными связями (LFSR) или регистров сдвига с нелинейными обратными связями (NLFSR) – $SR_i\,(i=1,\ldots,L)$. Функция f рассматривается как комбинирующая или фильтрующая функция от L переменных.

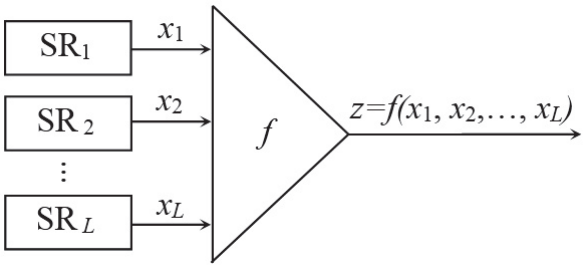

Рис. 1. Структурная схема комбинирующего генератора ПВП

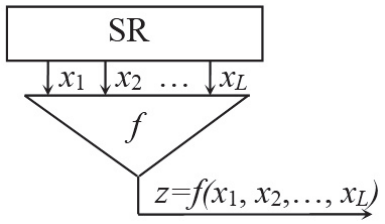

Рис. 2. Структурная схема фильтрующего генератора ПВП

Булевой функцией, которая соответствует NLFSR, в общем виде называется булево отображение вида $f: GF_2^L \to GF_2$. Булевые функции будем представлять в виде многочленов (поленом Жегалкина или алгебраическая нормальная форма – АНФ) над полем F_2:

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

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

Будем исследовать только те NLFSR, которые формируют модифицированную последовательность де Брейна (которая является последовательностью максимального периода, то есть М-последовательностью). Обозначим такие нелинейные регистры как M-NLFSR.

1.2. Изучаемые криптографические свойства M-NLFSR

Рассмотрим некоторые из основных, в данном случае, показателей оценки криптографической стойкости:

– *Сбалансированность.*

Булева функция f от L переменных называется сбалансированной, если функция принимает значение 0 и 1 одинаково часто. Это одно из наиболее естественных необходимых

свойств, накладываемых на булевы функции, которые используются в текущих шифрах [1].

Если булева функция сбалансирована, то вероятность того, что она примет значение 0 или 1, одинакова и равна 1/2. Это позволяет ослабить статистические зависимости между входом функции и ее выходом. В противном случае у криптоаналитика есть возможность, используя распределение всех соотношений, провести криптоанализ шифра.

– *Наличие запретов*.

В случае анализа ПСП, который генерируется с помощью фильтрующего генератора, возникает еще одно понятие – запрет булевой функции, то есть наличие комбинаций выходной последовательности, которая не может иметь место ни при каких комбинациях входной последовательности.

Интуитивно понятно, что наличие запрета в фильтрующей функции генератора делает ее «слабее», этот запрет никогда не появится в выходной последовательности генератора, которая ухудшает его статистические свойства.

– *Корреляционная иммунность*.

Требование корреляционной иммунной функции связано с противостоянием корреляционной атаке, идея которой заключается в следующем [2]. Рассмотрим комбинирующий генератор ПВП (рис. 1). Ключом генератора являются начальные состояния всех регистров. Объем ключа равен $2^{l_1+\ldots+l_L}$, где l_i – длина SR_i для $i=1,\ldots,L$.

Каждый из SR_i генерирует последовательность $x_i = x_i^1 x_i^2 \ldots$, как правило, близкую по своим свойствам случайно. В частности, при достаточно большой длине последовательности для случайно выбранного ее бита x_i^j имеет место вероятность случайного события $x_i^j = 0$: $\mathrm{P}[x_i^j = 0] \approx 1/2$. Итак, если $y = y^1 y^2 \ldots$ – произвольная последовательность, которая не зависит от x_i, то

$$\mathrm{P}[x_i^j = y^j] = \mathrm{P}[x_i^j = 0]\cdot\mathrm{P}[y^j = 0] + \mathrm{P}[x_i^j = 1]\cdot\mathrm{P}[y^j = 1] \approx \frac{1}{2}\left(\mathrm{P}[y^j = 0] + \mathrm{P}[y^j = 1]\right) = \frac{1}{2} \qquad (2)$$

Предположим, что $\mathrm{P}[f = x_1] \neq 1/2$ (в этом случае говорят, что функция f коррелирует с переменной x_1). С помощью корреляционной атаки найдем исходное состояние s_1 SR_1. Для этого будем перебирать все возможные 2^{l_1} состояний SR_1, для каждого из них строим последовательность $z' = z'_1 z'_2 \ldots$ и подсчитываем количество совпадений с ПВП $z'_i = z_i$. Для всех последовательностей, кроме одной (генерируемой s_1), доля совпадений будет $\approx 1/2$. Тем самым, определим, что часть ключа – состояние s_1. Если функция f имеет корреляцию со всеми своими переменными (или со всеми, кроме одной – тогда состояние регистра, соответствующего этой переменной, найдем последним, зная состояние всех остальных регистров), то найдем ключ генератора с $2^{l_1} + \ldots + 2^{l_L}$ испытаниями, что гораздо меньше сложности атаки грубой силы.

– *Нелинейность*.

Практика показывает [3], что криптографические преобразования, которые обладают свойствами, близкими к свойствам линейных функций, во многих случаях приводят к существенному снижению устойчивости шифров. По этой причине в криптографии важное значение имеют функции, свойства которых исключают слабости, присущие функциям, близким к линейным. Таким образом, желаемым качеством функции является ее нелинейность, что понимается в широком смысле как отрицание линейности. В блочных и поточных шифрах применения функции с высокой нелинейностью способствуют повышению устойчивости шифров к линейному и дифференциальному методам криптоанализа.

1.3. Постановка задачи

В литературе мало описывается связь между различными криптографическими свойствами. Практика показывает [1], что в качестве компонент шифра необходимо выбирать «хорошие со всех сторон» функции, что есть на самом деле очень непростой задачей, поскольку многие свойства противоречат друг другу. Хотя теоретические результаты показывают, что в случайной функции много криптографических параметров, близких к оптимальным. Вопрос в том, как ее выбрать?

Кроме оптимизации показателей криптографической стойкости, при практической реализации необходимо учитывать простоту реализации (как программной, так и аппаратной). Чем меньше ресурсов (памяти, количество элементарных операций – при программной реализации; логических элементов и возможность их распараллеливания – при аппаратной) затрачивается алгоритмом на формирование очередного бита, тем легче получить более быстродействующий, дешёвый в изготовлении и менее энергозатратный при использовании конечный продукт.

Работа является расширением материалов, полученных авторами и изложенных в [4] для случая использования АНФ с нелинейностью произвольного порядка. Для полноты изложения материала в данной работе приводятся результаты, изложенные в [4].

В статье анализируется возможность использования M-NLFSR в качестве комбинирующей или фильтрующей функции. Изучается вопрос оптимизации выбора M-NLFSR по критериям максимальной корреляционной иммунности и нелинейности при различной алгебраической степени и возможности минимизации количества используемых мономов.

1.4. Используемые определения

F_2 – конечное поле из двух элементов, 0 и 1;

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

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: $(a_1, a_2, \ldots, a_L)$, $(a_2, a_3, \ldots, a_{L+1})$, …, $(a_{2^L+L+1}, a_{2^L+L+2}, \ldots, a_{2^L})$, каждый из возможных кортежей присутствует и встречается ровно один раз, т.е. встречаются все возможные 2^L комбинации над алфавитом $\{0,1\}$ [5, 6].

Аналогичные последовательности $2^L - 1$ без кортежей из одних нулей называется *модифицированными последовательностями де Брейна*.

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

$$f(x) = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_L x_L \oplus b, \tag{3}$$

где $b \in F_2, a \in V_L$. Если $b = 0$, то функция называется линейной, а соответствующий ей регистр сдвига LFSR. Функция называется квадратичной, кубической и т.д., если ее алгебраическая степень соответственно 2, 3 и т.д. Функция с $\deg(f) = 1$ является аффинной. Случай, когда в аффинной функции $a_0 = 0$, соответствует линейной функции. Множество аффинных булевых функций от L переменных обозначается как A_L.

Весом Хэмминга или просто *весом* двоичного вектора называется число единиц среди его компонент. Вес Хэмминга булевой функции есть вес вектора ее значений. Вес вектора или функции обозначается как $wt(x)$ и $wt(f)$.

Расстояние Хэмминга $dist(f,g)$ между двумя функциями f и g есть вес функции $f \oplus g$. Другими словами, это число тех $x \in V_L$, на которых $f(x) \neq g(x)$.

Нелинейностью N_f булевой функции f называется расстояние Хэмминга между f и множеством аффинных функций.

Максимально нелинейной называется булева функция от L переменных (L любое) такая, что расстояние Хэмминга от данной функции до множества всех аффинных функций является максимально возможным. В случае четного L максимально возможное значение нелинейности равно $2^{L-1} - 2^{(L/2)-1}$. В случае нечетного L точное значение максимального расстояния неизвестно. Термин «максимально нелинейная функция» принят в отечественной литературе, тогда как в англоязычной широкое распространение получил термин «бент-функция». Аналогия между терминами неполная. При четном числе переменных L бент-функции и максимально нелинейные функции совпадают, а при нечетном L бент-функции (в отличие от максимально нелинейных) не существуют. Кроме того, все бент-функции не сбалансированы (в отличие от функций соответствующих M-NLFSR, как будет показано ниже), что делает их уязвимыми к статистическому анализу.

2. Полученные результаты

2.1. Сбалансированность

M-NLFSR, как и M-LFSR, генерируют модифицированную последовательность де Брейна, и если добавить к рассмотрению состояние заполнения всех ячеек нулевым значением, то полученная функция будет сбалансированной. При равновероятном и независимом выборе аргументов булевой функции f, которая образует M-NLFSR, вероятности ее значений, соответственно $P(1) = wt(f)/2^L$ $P(0) = 1 - wt(f)/2^L$.

2.2. Наличие запретов

M-NLFSR являются функциями, которые не имеют запретов. Это следует из того, что NLFSR формируют последовательность де Брейна, которая по определению имеет все возможные комбинации последовательности.

Однако следует быть осторожными, поскольку вполне сбалансированная фильтрующая функция в том или ином виде переносит свойства входной последовательности свойству последовательности, которая генерируется [7]. Например, в работе [8] установлен новый критерий, который идейно говорит следующее: «фильтрующая функция сохраняет запреты (в соответствующем смысле) тогда и только тогда, когда она полностью сбалансирована». Соответственно, если на вход функции поступает «далекая» от случайной последовательности, то и на выходе ее статистические свойства будут плохие.

2.3. Корреляционная иммунность

Приведенные в данном и следующем разделе утверждение и теоремы даны без доказательства с целью сокращения объема работы. Доказательства являются общедоступными и приведены, например, в [1 – 3, 9 – 12].

Наличие корреляционно иммунной функции степени m означает, что значения функции $Z = f(X)$ статистически независимы от любого набора с не более чем m компонентов произвольного вектора аргументов $X = (F_2)^L$. Это равнозначно условию, что на выход преобразования не «просачивается» информация о векторах, поступающих на вход преобразования и имеющих вес Хэмминга не более m.

Булева функция f называется корреляционно иммунного порядка m, $1 \le m \le L$, если для любой совокупности номеров m переменных $1 \le i_1 < i_2 < \ldots < i_m \le L$ случайные величины $X = \left(x_{i_1}, x_{i_2}, \ldots, x_{i_m}\right)$ и $Y = f\left(x_1, x_2, \ldots, x_L\right)$ являются независимыми.

Можно показать, что корреляционно иммунная порядка m функция от L переменных является корреляционно иммунной произвольного меньшего порядка. Таким образом, булевой функции f соответствует какой-либо максимальный порядок ее корреляционной иммунности $m_{\max}$, который обозначается $cor(f)$.

Случай, когда $m = L$ имеет место только когда $f = const$. Максимального корреляционного иммунитета степени $m = L - 1$ достигают только аффинные функции, то есть криптографически слабые. Кроме того, если f сбалансированная и $cor(f) = L - 2$, то функция f также аффинная. Таким образом, имеет смысл рассматривать порядок корреляционной иммунности m только в диапазоне $1 \le m \le L - 3$.

Сбалансированная корреляционно-иммунная функция порядка называется -стойку функцией. Формально, любую сбалансированную булеву функцию можно рассматривать как 0-стойку и произвольную булеву функцию как (-1) стойку. По аналогии с вводимым обозначения для максимального порядка устойчивости:

$$sut(f) = \begin{cases} -1, & \text{если } f \text{ не збалансированная,} \\ cor(f), & \text{если } f \text{ збалансированная.} \end{cases}$$

Неравенство Зигенталера. Если f – корреляционно-иммунная порядка m функция на $(F_2)^L$, то:

$deg(f) \le L - m$;

если f – сбалансированная и $sut(f) = m \le L - 2$, то $deg(f) + sut(f) \le L - 1$.

Неравенство Зигенталера является одним из многих противоречий криптографических свойств функций друг другу: высокий порядок корреляционной иммунной функции влечет ее низкую алгебраическую степень, и наоборот.

Если функция сбалансированная, $sut(f) = m \le L - 2$ и $\deg(f) = L - m - 1$, то f называется *m-оптимальной*. Откуда имеем m-оптимальные f для LFSR $m = L - 1 - \deg(f) = L - 2$ и для NLFSR второго порядка $m = L - 1 - \deg(f) = L - 3$ и т.д. Значение максимального порядка устойчивости для m-оптимальных функций, в зависимости от длины регистра и алгебраической степени, приведены в табл. 1.

Таблица 1

Значение максимального порядка устойчивости для m-оптимальных функций

	L						
	3	4	5	6	7	8	9
M-LFSR	1	2	3	4	5	6	7
M-NLFSR 2-го порядка	0	1	2	3	4	5	6
M-NLFSR 3-го порядка	–	0	1	2	3	4	5
M-NLFSR 4-го порядка	–	–	0	1	2	3	4

Таблица 2

Распределение количества регистров в зависимости от максимальной устойчивости для M-NLFSR

$sut(f)$	Количество M-LFSR	Количество M-NLFSR 2-го порядка	Количество M-NLFSR 3-го порядка	Количество M-NLFSR 4-го порядка
$L=2$				
m=0	0	–	–	–
m=1	1	–	–	–
$L=3$				
m=0	0	–	–	–
m=1	^{m}2	–	–	–
$L=4$				
m=0	0	4	–	–
m=1	2	^{m}10	–	–
m=2	0	–	–	–
$L=5$				
m=0	0	64	1024	–
m=1	2	52	^{m}896	–
m=2	0	^{m}6	–	–
m=3	^{m}4	–	–	–
$L=6$				
m=0	0	788	1434988	44586880
m=1	2	1044	640762	^{m}20424832
m=2	0	76	^{m}19450	–
m=3	4	^{m}38	–	–
m=4	0	–	–	–

Таблица 3

Распределение количества регистров в зависимости от максимальной устойчивости для M-PCHOC с $deg(f)\le 2$

$sut(f)$	Количество M-NLFSR	Количество M-LFSR	Количество M-NLFSR 2-го порядка
$L=7$			
m=0	33 988	0	33 988
m=1	25 582	4	25 578
m=2	4 090	0	4 090
m=3	388	10	378
m=4	4	0	^{m}4
m=5	4	^{m}4	–
$L=8$			
m=0	1 686 218	0	1 686 218
m=1	2 120 124	0	2 120 124
m=2	194 798	0	194 798
m=3	16 624	12	16 612
m=4	188	0	188
m=5	46	4	^{m}42
m=6	0	0	–
$L=9$			
m=0	284 956 836	0	284 956 836
m=1	208 843 950	2	208 843 948
m=2	24 325 344	0	24 325 344
m=3	1 091 584	16	1 091 568
m=4	21 192	0	21 192
m=5	876	28	848
m=6	10	0	^{m}10
m=7	2	^{m}2	

Таким образом, мы определили верхнюю границу значений для m-стойких функций. В работе исследованы корреляционная иммунность всего множества M-NLFSR размерностью $2 \le L \le 6$ (результаты представлены в табл. 2), а также M-LFSR и M-NLFSR 2-го порядка для $L \le 9$ (табл. 3). Как видно из табл. 2, 3, M-NLFSR достигают значения для m-оптимальных функций (в таблице обозначены как «^{m}») при всех изученных L. Однако есть очень большая доля (примерно половина всего множества M-NLFSR 2-го порядка при $7 \le L \le 9$ и 2/3 при $L = 6$), которая не имеет корреляционной иммунности.

2.4. Нелинейность

Нелинейностью функции f, как уже было сказано, называется расстояние от f к классу аффинных функций A_L:

$$N_f = dist(f, A_L) = \min_{g \in A_L} dist(f, g). \quad (4)$$

Следующие утверждения показывают, что чем выше порядок корреляционной иммунной функции, тем ниже верхний предел ее нелинейности.

Если f сбалансированная и m-стойкая, $m \le L-2$. Тогда $N_f \le 2^{L-1} - 2^{m+1}$.

По аналогии с понятием m-оптимальной функции вводится специальное название для m-устойчивой функции максимально возможной нелинейности.

Если функция f из $(F_2)^L$ сбалансированная, $sut(f) = m \le L-2$ и $N_f = 2^{L-1} - 2^{m+1}$, то f называется *m-насыщенной*.

В табл. 4 приведены рассчитанные значения максимально возможной нелинейности сбалансированной функции в зависимости от ее устойчивости.

Таблица 4

Значения нелинейности m-насыщенных функций в зависимости от их максимальной устойчивости

	$sut(f)$						
	0	**1**	**2**	**3**	**4**	**5**	**6**
$L=3$	2	0	–	–	–	–	–
$L=4$	6	4	0	–	–	–	–
$L=5$	14	12	8	0	–	–	–
$L=6$	30	28	24	16	0	–	–
$L=7$	62	60	56	48	32	0	–
$L=8$	126	124	120	112	96	64	0
$L=9$	254	252	248	240	224	192	128

Однако значения нелинейности, приведенные в табл. 4, не обязательно достижимы. Обозначим через $N_{f\max}(L,m)$ *максимально возможную нелинейность* m-стойкой булевой функции, заданной на $(F_2)^L$ и приведем верхнюю оценку для нелинейности m-стойких функций.

Из приведенного следует, что $N_{f\max}(L,-1) = 2^{L-1} - 2^{L/2-1}$ – это значение может достигаться только для четных L. Если f является сбалансированной функцией и L – четное значение, справедливо $N_{f\max}(L,m) = 2^{L-1} - 2^{L/2-1} - 2^{m+1}$ [2].

В [13] указывается, что для нечетных L и $L \le 7$, $N_{f\max}(L,-1) = 2^{L-1} - 2^{(L-1)/2}$, но для нечетных L и $L \ge 15$, справедливо неравенство $N_{f\max}(L,-1) > 2^{L-1} - 2^{(L-1)/2}$.

При $m \ge L-2$, согласно неравенству Зигенталера $\deg(f) \le 1$, откуда $N_{f\max}(L,m) = 0$. Также в [13] ссылаются на доказанное неравенство $N_{f\max}(L, L-3) = 2^{L-2}$ и

гипотезу, что $N_{f\max}(L, L-4) = 2^{L-1} - 2^{L-3}$. Кроме того, приведены некоторые точные значения $N_{f\max}(L,m)$ для малых L и m:

$N_{f\max}(4,0) = 4$;

$N_{f\max}(5,-1) = N_{f\max}(5,0) = N_{f\max}(5,1) = 12$;

$N_{f\max}(6,0) = 26$; $N_{f\max}(6,1) = N_{f\max}(6,2) = 24$;

$N_{f\max}(7,-1) = N_{f\max}(7,0) = N_{f\max}(7,1) = 56$.

Указанные результаты не противоречат результатам, полученным в данной работе и приведенным ниже.

Полученные нами результаты распределения по нелинейности всего множества M-РСНОС размерностью до $L \le 6$ сведены в табл. 5.

Таблица 5

Распределение количества регистров в зависимости от нелинейности

N_f	Количество M-LFSR	Количество M-NLFSR 2-го порядка	Количество M-NLFSR 3-го порядка	Количество M-NLFSR 4-го порядка
$L = 2$				
0	1			
$L = 3$				
0	2			
$L = 4$				
0	2			
4		14		
$L = 5$				
0	6			
4			296	
8		66	1624	
12		56		
$L = 6$				
0	6			
4				1 424
8			2 892	80 004
12			57 688	1 844 824
16		350	615 116	19 851 036
20			988 840	42 826 836
24		1 596	430 664	407 588

В табл. 6, 7 сведены результаты распределения для $L \le 6$ в зависимости от нелинейности и максимального порядка устойчивости, а в табл. 8, 9 – результаты для M- NLFSR 2-го порядка при $7 \le L \le 9$.

Таблица 6

Распределение количества регистров в зависимости
от нелинейности и максимальной устойчивости для M-NLFSR (при $L \le 6$ $\deg(f) = 1,2$)

N_f	Количество M-LFSR				Количество M-NLFSR 2-го порядка			
	$sut(f)$, при $m =$				$sut(f)$, при $m =$			
	0	1	2	3	0	1	2	3
$L = 2$								
0		1	–	–	–	–	–	–
$L = 3$								
0		m 2	–	–		–	–	–
$L = 4$								
0		2		–			–	–
4			–	–	41)	m 10	–	–
$L = 5$								
0		2		m 4				–
4				–				–
8				–	8	52	m 6	–
12			–	–	561)		–	–
$L = 6$								
0		2		4				
4								
8								
12								
16					48	188	76	m 38
20				–				–
24				–	740	8561)		–

Таблица 7

Распределение количества регистров в зависимости
от нелинейности и максимальной устойчивости для M-NLFSR (при $L \le 6$ $\deg(f) = 3,4$)

N_f	Количество M-NLFSR 3-го порядка			Количество M-NLFSR 4-го порядка	
	$sut(f)$, при $m =$			$sut(f)$, при $m =$	
	0	1	2	0	1
$L = 2$					
0	–	–	–	–	–
$L = 3$					
0	–	–	–	–	–
$L = 4$					
0	–	–	–	–	–
4	–	–	–	–	–
$L = 5$					
0			–	–	–
4	128	168	–	–	–
8	896	728	–	–	–
12			–	–	–
$L = 6$					
0					
4				652	772
8	516	2 030	346	46 484	33 520
12	57 688			1 132 844	711 980
16	201 388	397 360	16 368	13 341 932	6 509 104
20	988 840			29 715 620	13 111 216
24	186 556	241 372[1)]	m 2 736	349 348	58 240[1)]

Таблица 8

Распределение количества регистров в зависимости
от нелинейности и максимальной устойчивости для M-NLFSR (при $7 \le L \le 9$ $\deg(f) = 2$)

N_f	$sut(f)$, при $m =$		
	0	1	2
$L = 7$			
0	0	0	0
32	40	716	494
48	7 624	24 862	3 596
56	26 324[1)]	0	0
$L = 8$			
0	0	0	0
64	148	1 578	2 226
96	65 078	380 856	192 572
112	1 620 992	1 737 690	0
$L = 9$			
0	0	0	0
128	200	4398	6 608
192	498 196	4 872 526	4 953 980
224	67 714 544	203 967 024	19 364 756
240	216 743 896	0	0

Таблица 9

Распределение количества регистров в зависимости
от нелинейности и максимальной устойчивости для M-NLFSR (при $7 \le L \le 9$ $\deg(f) = 2$)

N_f	$sut(f)$, при $m =$			
	3	4	5	6
0	0	0	0	–
32	378	***m*** 4	–	–
48	0	–	–	–
56	–	–	–	–
0	0	0	0	0
64	2 342	188	***m*** 42	–
96	14 270	0	–	–
112	0	–	–	–
0	0	0	0	0
128	12 198	2 550	848	***m*** 10
192	1 079 370	18 642	0	–
224	0	0	–	–
240	0	–	–	–

Как видно из приведенных результатов, M-NLFSR одновременно достигают максимально возможную устойчивость и максимальную нелинейность. Причем, все *m*-оптимальные функции также являются и *m*-насыщенными (в табл. 6 – 9 отмечены значком «***m***»). Кроме того, многие M-NLFSR которые не являются ***m***-насыщенными функциями по определению, достигают максимально возможного результата для $N_{f\max}(L,m)$, приведенных выше (в табл. 6 – 9 отмечены значком «**1)**»).

Приведем некоторые из полученных нелинейных рекуррентных соотношений одновременно *m*-оптимальных и *m*-насыщенных функций соответствующих M-NLFSR:

для M-NLFSR второго порядка размерности $L=5$ (с нелинейностью N_f=8 и максимальной устойчивостью $sut(f)$=2, количество мономов – 6):

$$f=x_2+x_3+x_4+x_5+x_2\cdot x_3+x_1\cdot x_3$$
$$f=x_1+x_3+x_4+x_5+x_1\cdot x_4+x_1\cdot x_2$$
$$f=x_1+x_2+x_4+x_5+x_1\cdot x_4+x_3\cdot x_4$$
$$f=x_1+x_2+x_4+x_5+x_1\cdot x_4+x_1\cdot x_3$$
$$f=x_1+x_2+x_3+x_5+x_1\cdot x_4+x_1\cdot x_3$$
$$f=x_1+x_3+x_4+x_5+x_1\cdot x_4+x_2\cdot x_4$$

для M-NLFSR третьего порядка размерности $L=6$ (с нелинейностью N_f=24 и максимальной устойчивостью $sut(f)$=2, 70 функций по 10 мономов, 346 по 12 мономов, 1124 – 14 мономов, 924 – 16 мономов, 252 – 18 мономов, 20 – 20 мономов):

$$f=x_4+x_5+x_6+x_1\cdot x_2+x_1\cdot x_3+x_2\cdot x_3+$$
$$+x_3\cdot x_4+x_1\cdot x_2\cdot x_3+x_1\cdot x_3\cdot x_4+x_1\cdot x_3\cdot x_5$$
$$f=x_3+x_4+x_5+x_6+x_1\cdot x_2+x_1\cdot x_4+x_2\cdot x_5+$$
$$+x_1\cdot x_2\cdot x_3+x_1\cdot x_2\cdot x_4+x_1\cdot x_2\cdot x_5$$

для M-NLFSR второго порядка размерности $L=9$ (с нелинейностью N_f=128 и максимальной устойчивостью $sut(f)$=6, количество мономов – 10):

$$f=x_1+x_2+x_3+x_4+x_5+x_6+x_7+x_9+x_2\cdot x_5+x_2\cdot x_8$$
$$f=x_2+x_3+x_4+x_5+x_6+x_7+x_8+x_9+x_1\cdot x_7+x_4\cdot x_7$$
$$f=x_1+x_2+x_3+x_4+x_5+x_7+x_8+x_9+x_4\cdot x_6+x_4\cdot x_8$$
$$f=x_1+x_2+x_4+x_5+x_6+x_7+x_8+x_9+x_1\cdot x_5+x_3\cdot x_5$$
$$f=x_1+x_2+x_3+x_4+x_6+x_7+x_8+x_9+x_3\cdot x_5+x_3\cdot x_6$$
$$f=x_1+x_2+x_3+x_5+x_6+x_7+x_8+x_9+x_3\cdot x_6+x_4\cdot x_6$$
$$f=x_1+x_2+x_3+x_4+x_6+x_7+x_8+x_9+x_1\cdot x_6+x_5\cdot x_6$$
$$f=x_1+x_2+x_3+x_5+x_6+x_7+x_8+x_9+x_3\cdot x_4+x_3\cdot x_8$$
$$f=x_1+x_2+x_3+x_4+x_6+x_7+x_8+x_9+x_2\cdot x_7+x_5\cdot x_7$$
$$f=x_1+x_2+x_3+x_5+x_6+x_7+x_8+x_9+x_2\cdot x_4+x_2\cdot x_7$$

Анализируя полученные результаты, видим, что симметричные M-NLFSR имеют одинаковые показатели $sut(f)$ и N_f. Все изученные M-NLFSR с $\deg(f)\geq 2$ имеют $N_f\geq 2^{L-\deg(f)}$.

Выводы

Получено и исследовано полное множество M-NLFSR $2\leq L\leq 6$, а также с $7\leq L\leq 9$, имеющих алгебраическую степень формирующей АНФ не выше $\deg(f)\leq 2$.

Функции, соответствующие M-NLFSR, являются сбалансированными функциями и не имеют запретов.

Протестирована и определена их корреляционная иммунность и нелинейность. Приведено распределение количества M-NLFSR для разных значений корреляционной иммунности, нелинейности, алгебраической степени и числа мономов в АНФ.

Показано, что M-NLFSR достигают значений корреляционной иммунности, соответствующих m-оптимальным функциям при всех изученных L. Однако есть большая доля функций, которые не имеют корреляционной иммунности. Кроме того, функции могут быть одновременно m-оптимальными и m-насыщенными.

Приведен ряд m-оптимальных и одновременно m-насыщенных функций, соответствующих M-NLFSR, при этом обладающих минимальным количеством мономов АНФ, что позволяет на их основе (при заданных размерах) минимизировать затраты (временные и аппаратные) для генерации ПВП.

Список литературы:

1. Городилова А.А. От криптоанализа шифра к криптографическому свойству булевой функции // Прикладная дискретная математика. – 2016. – № 3(33). – С.16–44

2. Панкратова И.А. Булевы функции в криптографии : учеб. пособие. – Томск : Изд. Дом Томск. гос. ун-та, 2014. – 88 с.

3. Мухачев В.А., Хорошко В.А. Методы практической криптографии. – К. : ООО «Полиграф-Консалтинг», 2005. – 215 с

4. Потий А.В., Полуяненко Н.А. Расчет числа образующих полиномов для регистров сдвига с нелинейной обратной связью с нелинейностью произвольного порядка // Міжнар. наук. конф. питання оптимізації обчислень (ПОО-XLIV) Інституту кібернетики імені В.М. Глушкова НАН України, 26–29 вересня 2017 року. Хмельницька область, м. Кам'янець-Подільський.

5. Хачатрян Л.Г. Методы построения последовательностей де Брейна // Дискретна математика. – 1991. – Т. 3, вып. 4. – С. 62–78

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

7. Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В. Булевы функции в теории кодирования и криптологии ; 2-е изд. – Москва : МЦНМО, 2012. – 584с.

8. Смышляев С.В. О криптографических слабостях некоторых классов преобразований двоичных последовательностей // Прикладная дискретная математика. – 2010. – № 1. – С. 5–15.

9. Токарева Н. Н. Обобщения бент-функций. Обзор работ // Дискретный анализ и исследование операций. – 2010. – Т. 17, №1. – С.33-62

10. Токарева Н.Н. Нелинейные булевы функции : бент-функции и их обобщения. Издательство LAP LAMBERT Academic Publishing (Saarbrucken, Germany), 2011. – 180 с. ISBN: 978-3-8433-0904-2.

11. Агафонова И.В. Криптографические свойства нелинейных булевых функций. Семинар по дискрет. гармон. анализу и геометр. моделированию. – СПб. : DHA & CAGD, 2007. – С. 1–24.

12. Шевелев Ю.П. Дискретная математика. Ч. 1: Теория множеств. Булева алгебра (Автоматизированная технология обучения «Символ») : учеб. пособие. – Томск. гос. ун-т систем управления и радиоэлектроники, 2003. –118 с. ; Молдовян А.А. Криптография. Скоростные шифры. – БХВ-Петербург, 2002. – 496 с.

13. Таранников Ю.В. О корреляционно-иммунных и устойчивых булевых функциях. Математические вопросы кибернетики. – Москва : Физматлит, 2002. – Вып. 11. – С. 91–148.

Харьковский национальный
университет имени В.Н. Каразина;
АО «Институт информационных технологий», Харьков;
Национальный университет обороны Украины
имени Ивана Черняховского, Киев

Поступила в редколлегию 28.10.2018