УДК 621.391.7

СИНТЕЗ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ НА ОСНОВЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ де БРЁЙНА НАД ИЗОМОРФНЫМИ ПРЕДСТАВЛЕНИЯМИ ПОЛЯ *GF*(256)

Д. т. н. М. И. Мазурков, А. В. Соколов

Одесский национальный политехнический университет
Украина, г. Одесса
radiosquid@gmail.com

Разработаны методы синтеза криптографических S-блоков подстановки, позволяющие экономить ресурсы памяти на основе последовательностей де Брёйна, построенных над изоморфными представлениями поля GF(256). Показано, что они обладают практически приемлемыми показателями криптографического качества и обеспечивают экономию памяти в k раз.

Ключевые слова: S-блок подстановки, поле Галуа, m-последовательность, последовательность де Брёйна.

Современное направление развития средств вычислительной техники, приводящее к постоянному росту разрядности вычислительных устройств, диктует необходимость увеличения длины блока данных современных блочных шифров, что ведет к увеличению длины их основных элементов — криптографических *S*-блоков подстановки [1]. Рост длины *S*-блоков подстановки положительно сказывается на их криптографическом качестве: резко растет расстояние нелинейности, падает корреляционная связь выхода и входа, увеличиваются алгебраическая степень нелинейности и период возврата. Однако увеличение длины *S*-блоков подстановки также означает затруднение процесса их выбора в виду стремительного роста общего количества существующих блоков подстановки. Например, для двухбайтных блоков количество возможных биективных перестановок достигает значения $2^{16}!$, что для современных вычислительных устройств эквивалентно машинной бесконечности. Данное обстоятельство исключает возможность применения переборных методов и диктует необходимость исследования *S*-блоков подстановки малой длины с целью выработки регулярных правил построения криптографически качественных больших *S*-блоков подстановки.

Обратной стороной увеличения длины *S*-блоков подстановки также является стремительное увеличение памяти, необходимой для их хранения. Например, для хранения двухбайтного *S*-блока подстановки понадобится сохранить 16 таблиц истинности компонентных булевых функций длиной 65536 бит каждая, что эквивалентно 1048576 бит регистров процессора. Уже при четырехбайтном блоке подстановки данный показатель достигает 137438953472 бит≈17 Гбайт, что является более чем затруднительным для аппаратной реализации на микропроцессорных системах.

Решение задачи синтеза экономичных с точки зрения подсистемы памяти *S*-блоков подстановки на основе последовательностей де Брёйна [2], однако максимальный размер *S*-блока подстановки, которого позволяют достичь предложенные методы, равен $N=2^4$ (*S*-блока подстановки, ориентированные на криптоалгоритм ГОСТ 28147-89), что является недостаточным для синтеза современных шифров.

Построение больших, экономичных с точки зрения подсистемы памяти *S*-блоков подстановки, соответствующих основным критериям криптографического качества возможно на основе *q*-ичных последовательностей максимальной длины, или *m*-последовательностей, порождаемых регистрами сдвига с обратной связью, построенных по закону генераторного полинома $f(z)$.

Количество существующих первообразных (генераторных) полиномов степени k над каждым изоморфным подполем $GF(q)$ определяется по формуле

$$\left|f_q^k\right| = \frac{\varphi\left(q^k - 1\right)}{k}, \qquad (1)$$

где $\varphi(x)$ — фи-функция Эйлера.

Например, для поля Галуа $GF(16)$ существуют следующие изоморфные представления

$$GF(16) => GF\left(2^4\right) => GF\left(4^2\right). \quad (2)$$

Для построения $GF\left(2^4\right)$ существуют $\left|f_2^4\right| = 2$ первообразных полинома, неприводимых над полем $GF(2)$:

$$f_1(z) = z^4 + z + 1; \quad f_2(z) = z^4 + z^3 + 1. \quad (3)$$

Для построения поля $GF\left(4^2\right)$ существует $\left|f_4^2\right| = 4$ нормированных первообразных полинома, неприводимых над полем $GF(4) = [0,1,2,3]$, [3]

$$f_3(z) = z^2 + z + 2; \quad f_4(z) = z^2 + z + 3; \quad f_5(z) = z^2 + 2 \cdot z + 2; \quad f_6(z) = z^2 + 3 \cdot z + 3. \quad (4)$$

В табл. 1 содержатся упорядоченные элементы расширенных полей Галуа $GF(16)$, построенные по модулям первообразных полиномов (3), (4), представленные в виде степеней первообразного элемента $\theta = z$, в виде полиномов над полем $GF(4)$ или полем $GF(2)$ в виде четверичных или двоичных векторов.

Таблица 1

Элементы полей, построенных по модулям первообразных полиномов $f_1 \ldots f_6$

Степени $\theta = z$	Ненулевые элементы поля $GF\left(2^4\right)$				Ненулевые элементы поля $GF\left(4^2\right)$							
	$f_1(z)$		$f_2(z)$		$f_3(z)$		$f_4(z)$		$f_5(z)$		$f_6(z)$	
1	2	3	4	5	6	7	8	9	10	11	12	13
z^0	1	0001	1	0001	1	01	1	01	1	01	1	01
z^1	z	0010	z	0010	z	10	z	10	z	10	z	10
z^2	z^2	0100	z^2	0100	$z+2$	12	$z+3$	13	$2z+2$	22	$3z+3$	33
z^3	z^3	1000	z^3	1000	$3z+2$	32	$2z+3$	23	$z+3$	13	$z+2$	12
z^4	$z+1$	0011	z^3+1	1001	$z+1$	11	$z+1$	11	$z+2$	12	$z+3$	13
z^5	z^2+z	0110	z^3+z+1	1011	2	02	3	03	2	02	3	03
z^6	z^3+z^2	1100	z^3+z^2+z+1	1111	$2z$	20	$3z$	30	$2z$	20	$3z$	30
z^7	z^3+z+1	1011	z^2+z+1	0111	$2z+3$	23	$3z+2$	32	$3z+3$	33	$2z+2$	22
z^8	z^2+1	0101	z^3+z^2+z	1110	$z+3$	13	$z+2$	12	$2z+1$	21	$3z+1$	31
z^9	z^3+z	1010	z^2+1	0101	$2z+2$	22	$3z+3$	33	$2z+3$	23	$3z+2$	32
z^{10}	z^2+z+1	0111	z^3+z	1010	3	03	2	02	3	03	2	02
z^{11}	z^3+z^2+z	1110	z^3+z^2+1	1101	$3z$	30	$2z$	20	$3z$	30	$2z$	20
z^{12}	z^3+z^2+z+1	1111	$z+1$	0011	$3z+1$	31	$2z+1$	21	$z+1$	11	$z+1$	11
z^{13}	z^3+z^2+1	1101	z^2+z	0110	$2z+1$	21	$3z+1$	31	$3z+2$	32	$2z+3$	23
z^{14}	z^3+1	1001	z^3+z^2	1100	$3z+3$	33	$2z+2$	22	$3z+1$	31	$2z+1$	21

Каждый столбец двоичного (столбцы 3 и 5) и четверичного (столбцы 7, 9, 11 и 13) представления элементов поля является *m*-последовательностями периода $T = q^k - 1 = 4^2 - 1 = 15$.

Проведенные исследования показали, что существующее количество различных структур *m*-последовательностей при различных первообразных полиномах $f(z)$ и различных первообразных элементах θ определяется только количеством существующих в поле первообразных неприводимых полиномов.

Приведем *m*-последовательности, соответствующие первообразным полиномам $f_1 \ldots f_6$:

$$M = \begin{bmatrix} m_1 = \{0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1\}; \\ m_2 = \{0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1\}; \\ m_3 = \{0 \quad 1 \quad 1 \quad 3 \quad 1 \quad 0 \quad 2 \quad 2 \quad 1 \quad 2 \quad 0 \quad 3 \quad 3 \quad 2 \quad 3\}; \\ m_4 = \{0 \quad 1 \quad 1 \quad 2 \quad 1 \quad 0 \quad 3 \quad 3 \quad 1 \quad 3 \quad 0 \quad 2 \quad 2 \quad 3 \quad 2\}; \\ m_5 = \{0 \quad 1 \quad 2 \quad 1 \quad 1 \quad 0 \quad 2 \quad 3 \quad 2 \quad 2 \quad 0 \quad 3 \quad 1 \quad 3 \quad 3\}; \\ m_6 = \{0 \quad 1 \quad 3 \quad 1 \quad 1 \quad 0 \quad 3 \quad 2 \quad 3 \quad 3 \quad 0 \quad 2 \quad 1 \quad 2 \quad 2\}. \end{bmatrix} \tag{5}$$

На базе каждой *m*-последовательности возможно построение последовательности де Брейна [2, 4], на базе которой может быть построена кодирующая *Q*-последовательность, задающая структуру криптографического *S*-блока подстановки. Для этого в *m*-последовательность должен быть вставлен символ «0» путем конкатенации его с серией из $k-1$ символов «0», что задает последовательность де Брёйна. В случае конструкции (5) символ «0» может быть добавлен к любому другому символу «0», что возможно только для случая $k=2 \Rightarrow k-1=1$. Алгоритм построения *S*-блока подстановки с помощью последовательности де Брейна заключается в отображении каждой серии из k бит в соответствующий элемент кодирующей *Q*-последовательности, определяющей структуру криптографического *S*-блока подстановки. Например, на основе последовательности m_1 может быть построена последовательность $Q_1 = \{0,1,2,4,9,3,6,13,10,5,11,7,15,14,12,8\}$.

Таким образом, для хранения всего *S*-блока подстановки необходимо хранить лишь последовательность де Брейна (генотип), из которой с помощью элементарных операций может быть получена *Q*-последовательность (фенотип), что определяет экономию ресурсов памяти *S*-блоков подстановки на основе *m*-последовательностей, которая так же, как и в работе [2] достигает значения k раз.

Аналогично выражению (2), рассмотрим поле $GF(256)$, которое имеет следующие свои изоморфные представления

$$GF(256) => GF(2^8) => GF(4^4) => GF(16^2), \tag{6}$$

среди которых в поле $GF(2^8)$ имеется $\left|f_2^8\right|=16$ первообразных полиномов, в поле $GF(4^4)$ имеется $\left|f_4^4\right|=32$ неприводимых полинома, существующих над арифметикой умножения по модулю единственного первообразного полинома $f(x)=x^4+x^3+1$, а также в поле $GF(16^2)$, в котором имеются $\left|f_{16}^2\right|=64$ первообразных полинома, существующих над арифметиками умножения, определенными первообразными полиномами, представленными в выражениях (3), (4). Таким образом, количество существующих в поле $GF(256)$ различных структур *m*-последовательностей определяется количеством всех существующих первообразных полиномов над изоморфными представлениями рассматриваемого поля:

$$J=\left|f_2^8\right|+1\cdot\left|f_4^4\right|+6\cdot\left|f_{16}^2\right|=16+32+6\cdot 64=432. \tag{7}$$

Исследование криптографических свойств полученных *S*-блоков подстановки длины $N=256$ на основе *m*-последовательностей над изоморфными полями Галуа $GF(256)$ показывают их высокий уровень криптографического качества. В табл. 2 представлены следующие основные его показатели:

— абсолютное значение максимального элемента матрицы коэффициентов корреляции (столбец 3);

— количество нулей в матрице коэффициентов корреляции (столбец 4);

— расстояние нелинейности в смысле расстояния до аффинного кода (столбец 5);

— алгебраическая степень нелинейности (столбец 6);

— период возврата подстановочной конструкции в исходное состояние (столбец 7).

Данные табл. 2 подтверждают эффективность предложенного алгоритма построения больших, экономичных с точки зрения подсистемы памяти *S*-блоков подстановки.

Таблица 2

Криптографические характеристики экономичных *S*-блоков подстановки

Поле	Вид первообразного полинома	$\max\{r_{i,j}\}$	K^0	N_s	$\min\{\deg(F_i)\}$	T
$GF(2^8)$	$\{\lvert f_2^8\rvert = 16\}$	0.0781…0.1250	1…10	100…106	7	70…56760
$GF(4^4)$	$\{\lvert f_4^4\rvert = 32\}$	0.0781…0.1563	1…16	96…106	6…7	9…224952
$GF(16^2)$	$\{z^4+z+1\}$, $\{\lvert f_{16}^2\rvert = 64\}$	0.0781…0.1406	1…17	92…104	6…7	3…41076
$GF(16^2)$	$\{z^4+z^3+1\}$, $\{\lvert f_{16}^2\rvert = 64\}$	0.0781…0.1563	1…9	92…104	6…7	5…20928
$GF(16^2)$	$\{z^2+z+2\}$, $\{\lvert f_{16}^2\rvert = 64\}$	0.0938…0.1563	1…16	92…104	6…7	15…140760
$GF(16^2)$	$\{z^2+z+3\}$, $\{\lvert f_{16}^2\rvert = 64\}$	0.0938…0.1563	1…11	92…104	6…7	2…289380
$GF(16^2)$	$\{z^2+2\cdot z+2\}$, $\{\lvert f_{16}^2\rvert = 64\}$	0.0938…0.1563	1…8	92…106	6…7	3…40128
$GF(16^2)$	$\{z^2+3\cdot z+3\}$, $\{\lvert f_{16}^2\rvert = 64\}$	0.0781… 0.1563	1…14	92…104	6…7	2… 26412

Отметим основные результаты проведенных исследований:

1. Использование полных семейств изоморфных полей Галуа позволяет построение множеств *m*-последовательностей применимых для формирования экономичных *S*-блоков подстановки, причем объем выигранной памяти растет с ростом длины *S*-блока подстановки и составляет k раз.

2. Криптографическое качество полученных экономичных *S*-блоков подстановки соответствует основным предъявленным к нему критериям. Причем улучшение показателей криптографического качества происходит пропорционально длине исходной *m*-последовательности.

3. Количество построенных экономичных *S*-блоков подстановки достаточно велико и составляет $J=432$, а также может быть увеличено за счет использования всех циклических сдвигов *Q*-последовательности без существенных потерь в криптографическом качестве.

Таким образом, в работе предложен конструктивный алгоритм построения экономичных с точки зрения подсистемы памяти криптографически качественных *S*-блоков подстановки, который может быть применен для синтеза нелинейных преобразований современных шифров.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Ростовцев А. Г. Большие подстановки для программных шифров // Проблемы инф. безопасности. Компьютерные системы.— СПб.— 2000.— № 3.— С. 31—34.

2. Мазурков, М. И., Соколов А. В. Методы синтеза двоичных псевдослучайных последовательностей со свойством k-граммного распределения.— Одесса: Труды ОНПУ.— 2012.— С.188 — 198.

3. Мазурков М. И., Конопака Е. А Семейства линейных рекуррентных последовательностей на основе полных множеств изоморфных полей Галуа // Радиоэлектроника. — 2005.— № 11.— С. 58 — 65. (Изв. вузов).

4. De Bruijn N. G. A combitorial problem // Nederl. Akad. Wetensch. Proc.— 1946.— Vol. 49.— P. 758—764.

M. I. Mazurkov, A. V. Sokolov

Nonlinear transformations based on the de Bruijn sequences built over isomorphic representations of GF(256) Galois field.

The synthesis methods of cryptographic substitution S-boxes, wich allow to save memory resources, basrd on de Bruijn sequences built over isomorphic representations of GF(256) Galois field have been developed. It is shown that they have practice-relevant performance of cryptographic quality and reduces memory usage by a factor of k.

Keywords: *substitution S-box, Galois field, m-sequence, de Bruijn sequence.*