

Т Р У Д Ы

XIV МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ
**СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ
И ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ**

27—31 мая 2013 г.
Украина, г. Одесса

Том I

Т Р У Д И

XIV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СУЧАСНІ ІНФОРМАЦІЙНІ ТА ЕЛЕКТРОННІ ТЕХНОЛОГІЇ

27—31 травня 2013 р.
Україна, м. Одеса
Том I

PROCEEDING

OF THE XIVth INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE
MODERN INFORMATION AND ELECTRONIC TECHNOLOGIES

27—31 May, 2013
Ukraine, Odessa

Volume I

<i>В. М. Дмитриев, Т. Н. Зайченко, Ю. А. Шурыгин.</i> Моделирование технических средств автоматизации и управления на базе метода компонентных цепей	157
<i>С. А. Положаенко, Омар Муаяд Абдуллах.</i> Мультимедийная информационная технология реализации средств математического моделирования диффузионных процессов	161
<i>С. А. Положаенко, Ю. В. Григоренко.</i> Математичні моделі процесів та апаратів первинної обробки сирих вуглеводнів	163
<i>Г. В. Шаповалов.</i> Разработка программного комплекса для исследования оптимального расположения элементов электронной техники в трехмерном пространстве	165
<i>В. А. Тудоран.</i> Двумерное моделирование погружения жесткого контура произвольной формы с учетом брызговой струи по схеме Эйлера—Лагранжа	167
<i>Г. М. Гайдаржи, А. С. Чебаненко, В. С. Ситников.</i> Диверсификация методов анализа и обработки нестационарных рядов на основе самообучающейся нейронной сети	170
<i>А. В. Никорак, А. А. Саченко, А. Ю. Роцупкин.</i> Усовершенствованная подсистема стабилизации и маневрирования мобильного балансирующего робота	172
<i>К. В. Зацелкин, В. В. Калинин, Н. О. Ульченко.</i> Комбинированный способ навигации автономного мобильного робота	174
<i>В. С. Ситников, Т. П. Яценко, А. М. Теплечук, І. С. Флоренко.</i> Реалізація управління перебудовою вузла фільтрації у спеціалізованій комп'ютерній системі управління автомобільним двигуном	178

Секция 2

Защита информации в широкополосных системах и компьютерных сетях

<i>А. А. Кобозева, О. В. Николаенко, В. С. Васьковец.</i> Преобразование спектра симметричной матрицы как возможная основа стеганографического алгоритма для произвольного цифрового изображения-контейнера	182
<i>И. И. Бобок, А. А. Кобозева.</i> Алгоритм выявления нарушения целостности цифрового изображения	184
<i>Б. В. Хлопов, Ю. С. Бондарев, Б. С. Лобанов, А. В. Шпак, А. Ю. Митягин.</i> Устойчивость магнитных свойств материалов НЖМД при воздействии на них внешних магнитных полей	186
<i>Б. С. Лобанов, Б. В. Хлопов, М. И. Самойлович, А. В. Шпак, А. Ю. Митягин, Я. Д. Ковалюк.</i> Электромагнитная восприимчивость композитных метаматериалов на основе опаловых матриц в системах уничтожения информации	188
<i>А. Я. Кулик, Ю. Ю. Иванов.</i> Застосування гіперболічних функцій для роботи з турбокодами у розподілених комп'ютерних системах різного функціонального призначення	190
<i>М. А. Мельник.</i> Стеганографический алгоритм для контейнеров-изображений, устойчивый к атаке сжатием	193
<i>Н. И. Куширенко, В. Я. Чечельницкий.</i> Аппаратный генератор перестановок	195
<i>Р.М.Пелещак, А.А.Вельченко, С.А.Вельченко.</i> Защита автоматизированной информационной системы с квантовым поляризационным кодированием на основе технологии плавающего кода	197
<i>А. С. Сафронов, Н. А. Барабанов, Ю. И. Венедиктов.</i> Анализ процессов развития систем информационной безопасности организации	201
<i>А. В. Соколов.</i> Множество нелинейных преобразований на основе конструкции Ниберг длиной $N=256$	204
<i>М. И. Мазурков, А. В. Соколов.</i> Синтез нелинейных преобразований на основе последовательностей де Брёйна над изоморфными представлениями поля $GF(256)$	208
<i>О. О. Цисар, К. В. Зацолкин.</i> Методика приховування даних, яка заснована на використанні клітинно-автоматного підходу	212
<i>К. В. Зацелкин, А. И. Иващенко, Е. Н. Иванова.</i> Усовершенствование метода скрытия данных Куттера—Джордана—Боссена	214

УДК 621.391.7

**СИНТЕЗ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ НА ОСНОВЕ
ПОСЛЕДОВАТЕЛЬНОСТЕЙ де БРЭЙНА 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 \approx 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

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

где $\varphi(x)$ — фи-функция Эйлера.

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

$$GF(16) \Rightarrow GF(2^4) \Rightarrow GF(4^2). \quad (2)$$

Для построения $GF(2^4)$ существуют $|f_2^4|=2$ 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 $GF(4^2)$ существует $|f_4^2|=4$ 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 $f_1 \dots f_6$

Степени $\theta = z$	Ненулевые элементы поля $GF(2^4)$				Ненулевые элементы поля $GF(4^2)$							
	$f_1(z)$		$f_2(z)$		$f_3(z)$		$f_4(z)$		$f_5(z)$		$f_6(z)$	
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 -последовательностью 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 $f_1 \dots f_6$:

$$M = \begin{cases} m_1 = \{0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1\}; \\ m_2 = \{0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1\}; \\ m_3 = \{0 & 1 & 1 & 3 & 1 & 0 & 2 & 2 & 1 & 2 & 0 & 3 & 3 & 2 & 3\}; \\ m_4 = \{0 & 1 & 1 & 2 & 1 & 0 & 3 & 3 & 1 & 3 & 0 & 2 & 2 & 3 & 2\}; \\ m_5 = \{0 & 1 & 2 & 1 & 1 & 0 & 2 & 3 & 2 & 2 & 0 & 3 & 1 & 3 & 3\}; \\ m_6 = \{0 & 1 & 3 & 1 & 1 & 0 & 3 & 2 & 3 & 3 & 0 & 2 & 1 & 2 & 2\}. \end{cases} \quad (5)$$

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 Брейна. 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 $Q = \{0, 1, 2, 4, 9, 3, 6, 13, 10, 5, 11, 7, 15, 14, 12, 8\}$.

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

$$GF(256) \Rightarrow GF(2^8) \Rightarrow GF(4^4) \Rightarrow GF(16^2), \quad (6)$$

среди которых в поле $GF(2^8)$ имеется $|f_2^8|=16$ первообразных полиномов, в поле $GF(4^4)$ имеется $|f_4^4|=32$ 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 $|f_{16}^2|=64$ 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:

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

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.

Криптографические характеристики экономичных S -блоков подстановки

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

М. И. Mazurkov, А. 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.*