УДК 681.3.06

МАЗУРКОВ М.И., СОКОЛОВ А.В.

АЛГОРИТМ СИНТЕЗА ЭКОНОМИЧНЫХ СХЕМ S-БЛОКОВ ПОДСТАНОВКИ НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

Одесский национальный политехнический университет,
Украина, Одесса, 65044, пр. Шевченко 1

Аннотация. Предложен алгоритм синтеза экономичных схем S-блоков подстановки на основе клеточных автоматов, которые удовлетворяют основным критериям криптографического качества. Найдены правила клеточных автоматов, позволяющие получить S-блоки подстановки, удовлетворяющие критерию максимального лавинного эффекта.
Ключевые слова: клеточный автомат, S-блок подстановки, максимальный лавинный эффект.

Abstract. A synthesis algorithm of efficient S-boxes based on cellular automata that satisfy the basic criteria of cryptographic quality is proposed. Cellular automata rules that allow obtaining S-boxes satisfying the criterion of maximum avalanche effect are found.
Keywords: cellular automata, S-box, maximum avalanche effect.

Вопросам конструирования криптографических биективных S-блоков подстановки, которые являются основными элементами современных блочных шифров, посвящено большое количество работ исследователей в области криптографии [1…3]. Современные методы конструирования высококачественных S-блоков подстановки подразумевают использование аппарата булевых функций для их описания [4]. Это позволяет достичь строго обоснованного уровня качества, которое определяется соответствием компонентных булевых функций конструируемого S-блока подстановки определенным критериям. К таким критериям качества относятся: высокая нелинейность, корреляционная независимость векторов выхода S-блока подстановки от его входа, строгий лавинный критерий, величина периодов возврата S-блока подстановки в исходное состояние. Однако, все чаще к требованиям конструируемых S-блоков подстановки относят критерий простоты их аппаратной или программной реализации [3]. Данное требование связано не только с концепцией энергоэффективности, но также с тем фактом, что с ростом длины S-блока подстановки существенно улучшаются все его показатели криптографического качества [5]. Возможность реализовать S-блок подстановки большей длины при том же количестве аппаратных средств и энергоэффективности ведет к существенному улучшению характеристик криптоалгоритма, в котором такой S-блок подстановки применяется.

Так, например, в случае использования криптографического S-блока подстановки, длина входного слова которого будет равна $k = 32$ бита, потребуется хранить в памяти криптографической системы кодирующую Q-последовательность, определяющую структуру S-блока подстановки, длины $N = 2^k = 2^{32} = 4294967296$. При этом, каждый элемент Q-последовательности представляет собой 32-разрядное число, т.е. необходимое для хранения S-блока подстановки количество памяти составит $4294967296 \cdot 32 = 137438953472$ бит $= 16$ ГБ, что является весьма существенным. При этом дальнейшее увеличение длины S-блока подстановки, происходящее в современных криптографических системах, приводит к экспоненциальному росту количества памяти, затрачиваемой на хранение Q-последовательности.

Данный факт делает актуальной задачу разработки новых схем реализации S-блоков подстановки большóй длины. В настоящий момент известен подход к построению экономичных S-блоков подстановки, основанный на особенностях конструкции Ниберг [6], а также подход на основе шумоподобных сигналов — последовательностей де Брейна

[3]. Тем не менее, и первый, и второй подходы являются эффективными только лишь при небольших значениях длины N S-блоков подстановки. Более перспективным и универсальным является новый подход к формированию S-блоков подстановки на основе математического аппарата клеточных автоматов, предложенный и обоснованный в [7].

Тем не менее, существенным недостатком сконструированных в [7] S-блоков подстановки является их небиективность, что ведет к трудностям в определении обратного преобразования и, несомненно, препятствует использованию эффективных схем S-блоков подстановки на основе клеточных автоматов на практике.

Целью настоящей статьи является разработка алгоритма синтеза биективных экономичных схем криптографических S-блоков подстановки на основе аппарата клеточных автоматов.

Рассмотрим криптографический S-блок подстановки, структура и свойства которого могут быть полностью заданы кодирующей Q-последовательностью [3,4], например, длины $N=16$

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

Для S-блока подстановки на основе (1) в соответствии с подходом к исследованию криптографических свойств с помощью аппарата булевых функций, могут быть записаны таблицы истинности компонентных булевых функций $f_1 \dots f_4$.

Таблица 1

Q	5	2	15	10	6	13	7	4	14	0	1	3	12	8	9	11
f_1	1	0	1	0	0	1	1	0	0	0	1	1	0	0	1	1
f_2	0	1	1	1	1	0	1	0	1	0	0	1	0	0	0	1
f_3	1	0	1	0	1	1	1	1	1	0	0	0	1	0	0	0
f_4	0	0	1	1	0	1	0	0	1	0	0	0	1	1	1	1

Очевидно, что объем памяти для хранения S-блока подстановки определяется суммой длин его компонентных булевых функций и существенно растет с ростом длины N S-блока подстановки.

Рассмотрим основные критерии криптографического качества, которые возможно измерить основываясь на представлении S-блока подстановки с помощью его компонентных булевых функций (табл.1) [8].

Очевидно, представленный S-блок подстановки является биективным, т.е. каждое число из диапазона $0,\dots,N-1$ встречается в его кодирующей Q-последовательности точно один раз. Свойство биективности криптографического S-блока подстановки приводит к тому, что все его компонентные булевы функции $f_1 \dots f_4$ являются сбалансированными, т.е. количество символов "1" в них равно количеству символов "0".

Важнейшим критерием качества S-блоков подстановки является максимизация его расстояния нелинейности [4], определяемого минимальным расстоянием от его компонентных булевых функций до аффинного кода $\varphi=\langle a,x\rangle+b$ (кода Рида-Маллера первого порядка)

$$N_S=\max\left\{\min_{i,j}\left\{dist(F_i,\varphi_j)\right\}\right\},\ i=0,1,\dots,k-1,\ j=0,1,\dots,2^{k+1}-1, \quad (2)$$

причем высокое расстояние нелинейности свидетельствует о высоком качестве криптографического S-блока подстановки, о трудности его аппроксимации множеством аффинных функций и, соответственно, бóльшей устойчивости к атакам линейного криптоанализа. Другим важным критерием, иллюстрирующим нелинейность S-блока подстановки является алгебраическая степень нелинейности — минимальная алгебраическая степень $\deg(\Phi_i)$ его компонентных булевых функций Φ_i, записанных с помощью полиномов Жегалкина [9].

Корреляционная взаимосвязь векторов выхода и входа S-блока подстановки определяется матрицей коэффициентов корреляции [3,4] векторов выхода y_j и векторов входа x_j $R = \| r_{\nu,\mu} \|$, где коэффициенты корреляции

$$r_{\nu,\mu} = 1 - 2^{-(k-1)} \sum_{z=1}^{N} \left(x_{z,\nu} \oplus y_{z,\mu} \right) = 0, \quad \nu, \mu = 1, 2, ..., k. \tag{3}$$

Лавинный эффект S-блока подстановки считается наилучшим, если для него выполняется строгий лавинный критерий (SAC) [2], т.е. производные каждой его компонентной булевой функции $D_{i,\nu} = f_i(x) \oplus f_i(x \oplus e_\nu)$ по всем направлениям e_ν веса $wt(e_\nu) = 1$ являются сбалансированными

$$wt\left(D_{i,\nu}\right) = 2^{k-1}, \; i, \nu = 0, 1, ..., k-1. \tag{4}$$

Смысловая трактовка выражения (4) заключается в том, что изменение любого входного бита компонентной булевой функции f_i ведет к изменению её выходного значения с вероятностью $P = 1/2$.

Период возврата S-блока подстановки в исходное состояние — наименьшее общее кратное $T = \text{НОК}(z_1, z_2 ...)$, где z_ξ — соответствующие длины циклов, на которые раскладывается Q-последовательность [10].

Рассмотрим подход к построению экономичных схем криптографических S-блоков подстановки, соответствующих приведенным критериям, на основе клеточных автоматов [7].

В простейшем случае одномерным клеточным автоматом называется дискретная структура, включающая в себя решетку ячеек памяти длины l, такую, что для каждой ячейки определена окрестность из r ячеек, взаимодействующих по правилу P, определяющему переход ячеек из текущего состояния — в новое с течением дискретного времени t.

Пусть, например, задано исходное состояние клеточного автомата, играющее роль входного слова однобайтного S-блока подстановки $x = \{1, 0, 0, 0, 1, 0, 1, 1\}$, окрестность $r = 1$, а также правило, для удобства представленное в виде следующей алгебраической конструкции [7]

$$P = \begin{array}{|c|c|c|c|c|c|c|c|} \hline 111 & 110 & 101 & 100 & 011 & 010 & 001 & 000 \\ \hline 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ \hline \end{array}, \tag{5}$$

где следует отметить, что для функционирования клеточного автомата, в памяти должна храниться только нижняя последовательность из (5), или собственно правило работы

автомата. На рис. 1 показано преобразование данных внутри клеточного автомата за один период дискретного времени под воздействием правила (5).

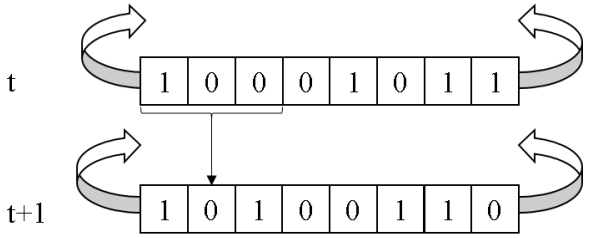

Рис. 1

Таким образом, когда входной вектор x пробегает все $N = 2^8 = 256$ значений получаем таблицу замены, являющуюся каноническим представлением S-блока подстановки в виде кодирующей Q-последовательности.

Отметим тот важнейший факт, что для реализации такого S-блока подстановки на основе клеточного автомата в памяти достаточно хранить только само правило, длина которого при значении окрестности $r = 1$ составляет всего 8 бит. Тогда как для хранения самой Q-последовательности потребовалось бы хранить все её 256 элементов разрядности 8 каждый, т.е. $256 \cdot 8 = 2048$ бит. Таким образом, применение математического аппарата клеточных автоматов позволяет добиться значительного выигрыша в необходимом для хранения S-блока подстановки количестве ячеек памяти, в указанном случае численно равного $\gamma = 2048/8 = 256$ раз.

Подобная идея реализации S-блоков подстановки рассматривалась в [7], однако, как было указано ранее, все разработанные подстановочные конструкции, несмотря на высокие показатели криптографического качества, являлись небиективными, что делало невозможным их применение во многих приложениях криптографии. В настоящей статье установлено, что получение биективных S-блоков подстановки возможно только при некоторых требованиях, предъявленных к правилу клеточного автомата. Сформулируем данные требования в виде двух свойств.

Свойство 1. Построить биективный S-блок подстановки на основе клеточного автомата возможно, только если двоичное представление правила P является сбалансированным.

Свойство 2. Если данное правило позволяет построить биективный S-блок подстановки при данном числе шагов дискретного времени t, то S-блок подстановки будет биективным при любом числе шагов.

Основываясь на приведенных свойствах, несложно найти подходящие правила, например, для длины входного слова S-блока подстановки $k = 8$ и окрестности $r = 1$

$$P = \begin{Bmatrix} 1,1,1,1,0,0,0,0 \\ 1,1,0,0,1,1,0,0 \\ 1,0,1,0,1,0,1,0 \\ 1,0,0,1,0,1,1,0 \\ 0,1,1,0,1,0,0,1 \\ 0,1,0,1,0,1,0,1 \\ 0,0,1,1,0,0,1,1 \\ 0,0,0,0,1,1,1,1 \end{Bmatrix}. \qquad (6)$$

Тем не менее, проведенные исследования позволили установить, что S-блоки подстановки, построенные на основе данных правил являются аффинными, т.е. совершенно неустойчивыми к атакам линейного криптоанализа.

Установлено, что для устранения данного недостатка могут быть использованы клеточные автоматы с бóльшим размером окрестности, например $r = 2$, а также более сложная схема коммутации входов и выходов клеточного автомата, изображенная на рис.2.

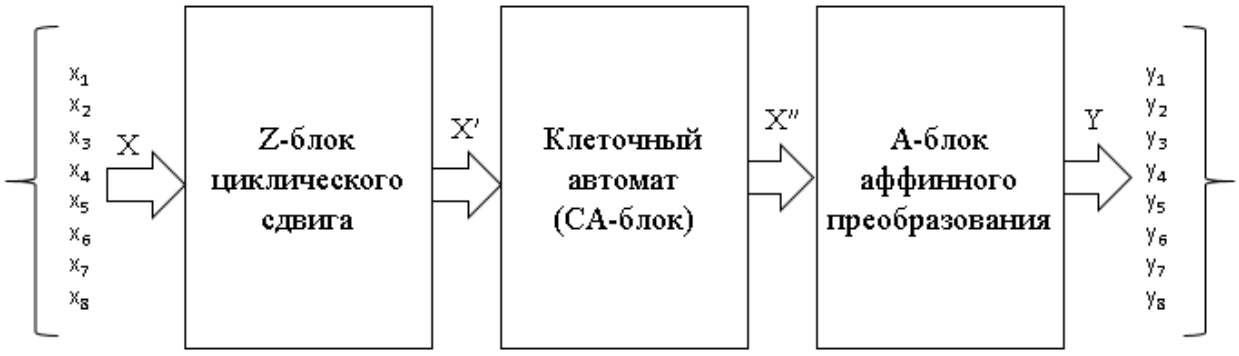

Рис. 2

На рис. 2 приняты следующие условные обозначения: $\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$ — входное слово криптографического S-блока подстановки; $\{y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8\}$ — выходное слово S-блока подстановки.

Z-блок циклического сдвига представляет собой предварительное преобразование входного слова путем его циклического сдвига вправо (влево при дешифровании) на определенную величину. Проведенные эмпирические исследования позволили установить оптимальную динамически изменяемую величину циклического сдвига Z, позволяющую получить наилучшие показатели криптографического качества

$$Z = s \bmod 3, \tag{7}$$

где s — десятичное представление 8-ми битного входного слова $\{x_i\}$, $i = 1, 2, ..., 8$. При этом, несмотря на то, что данное преобразование является динамическим, оно полностью обратимо.

A-блок аффинного преобразования представляет собой произведение вектора входных данных на матрицу аффинного преобразования, выполненное над полем $GF(2)$

$$Y = A \cdot X'' + a, \quad a \in GF(2), \tag{8}$$

где A — матрица аффинного преобразования. Выбор конкретного вида матрицы аффинного преобразования может осуществляться таким образом, чтобы были достигнуты наилучшие периоды возврата S-блока подстановки в исходное состояние, либо с помощью регулярного алгоритма, например, [11], позволяющего S-блоку подстановки достигнуть соответствия критерию максимального лавинного эффекта.

Важной задачей для построения высококачественного S-блока подстановки, соответствующего основным критериям криптографического качества, является выбор конкретного вида правила P работы клеточного автомата. При окрестности $r = 2$ и длине входного слова S-блока подстановки $k = 8$, длина правила составляет, соответственно, 32 бита. Построим таблицу, содержащую значения основных показателей криптографического качества для S-блоков подстановки на основе клеточных автоматов,

работающих на основе различных правил (табл. 2), выбрав число шагов $t = 3$. Для краткости, правила переходов записаны в виде десятичных эквивалентов.

Таблица 2

№ п/п	Правило P	N_s	$\deg(\Phi_i)$	$\max\{r_{v,\mu}\}$	$\min\{wt(D_{i,v})\}$	T	Ω
1	65535	84	7	0.0156	124	8	0
2	**851955**	**100**	**7**	**0.0625**	**112**	**32**	**5**
3	16711935	84	7	0.0156	124	8	0
4	16713975	86	7	0.0781	116	16	0
5	16716015	90	7	0.0938	112	80	0
6	16728255	90	7	0.0313	108	80	0
7	50135295	90	7	0.0313	108	80	0
8	150405375	90	7	0.0938	112	80	0
9	252645135	84	7	0.0156	124	8	0
10	252648975	92	7	0.0625	112	8	0
11	260509455	92	7	0.0625	112	8	0
12	267448335	78	7	0.0469	116	8	0
13	284098815	86	7	0.0781	116	16	0
14	**805359615**	**100**	**7**	**0.0625**	**112**	**32**	**5**
15	1431655765	84	7	0.0156	124	8	0
16	1431917913	98	7	0.0938	112	1232	0
17	1437248085	82	7	0.0469	116	4	0
18	1515890085	76	7	0.0313	108	8	0
19	1700095317	98	7	0.0938	112	1232	0
20	1718000025	82	7	0.0469	116	4	0
21	2576967270	82	7	0.0313	116	8	0
22	2594871978	90	7	0.2969	100	8	9
23	2779077210	76	7	0.0469	108	8	0
24	2857719210	82	7	0.0313	116	8	0
25	2863049382	90	7	0.2969	100	8	9
26	2863311530	84	7	0.3438	124	8	0
27	3489607680	94	7	0.2656	112	8	0
28	4042318320	88	7	0.3125	112	8	8905
29	4042322160	84	7	0.3438	124	8	0
30	4144561920	88	7	0.3125	116	16	0
31	4244832000	88	7	0.3125	116	8	0
32	4278239040	88	7	0.3125	116	8	0
33	4278251280	88	7	0.3125	116	16	0
34	4278253320	88	7	0.3125	112	8	0
35	4278255360	84	7	0.3438	124	4	0
36	4294115340	94	7	0.2656	112	8	0
37	4294901760	84	7	0.3438	124	8	0

В табл.2 под Ω понимается количество аффинных преобразований, приводящих к максимальному лавинному эффекту.

Определение. Нелинейный S-блок подстановки соответствует критерию максимального лавинного эффекта, если веса $wt(D_{i,k})$ всех производных его

компонентных булевых функций по всем направлениям единичного веса имеют значения, равные не менее половины длины S-блока [11]

$$wt\left(D_{i,\nu}\right) \geq N/2 = 128\,,\ i,\nu = 1,2,...,8\,. \tag{9}$$

В [11] предложен регулярный алгоритм синтеза матриц аффинного преобразования A, обеспечивающих максимальный лавинный эффект S-блока подстановки. Для полноты изложения материала статьи кратко рассмотрим этот алгоритм. Пусть, например, задан S-блок подстановки на основе клеточных автоматов, построенный в соответствии с правилом

$$P = 851955 = \{0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,1,1,1,1,1,1,1,1,1,1,1,0,0,1,1\}\,, \tag{10}$$

для которого, в соответствии с табл.2 существуют матрицы аффинного преобразования, приводящие к максимальному лавинному эффекту. Приведем таблицу замены данного S-блока подстановки в виде следующей алгебраической конструкции

S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	FF	EB	F5	43	AF	EF	86	DC	D7	B5	7F	C3	0D	2A	6E	A7
1	BE	11	6B	67	BF	47	1E	AB	1A	CF	15	72	73	C0	4F	2E
2	5F	B6	88	7E	D6	BD	B3	8D	FD	7B	8E	4D	0F	16	5D	E3
3	34	76	E7	66	A8	26	E4	38	B9	6C	06	95	9E	2D	17	46
4	FA	FB	6D	8A	44	D1	F3	30	AD	6F	DE	85	9D	89	1B	4B
5	FE	74	DB	62	1D	AA	A6	E5	78	9A	2C	08	AE	97	1F	92
6	68	E1	3B	4E	3F	6A	CC	CA	54	B0	31	40	C9	20	1C	A0
7	CD	BA	D8	83	03	5E	AC	77	3D	7C	96	05	B8	4A	8C	48
8	7D	A1	DF	9B	DA	87	45	D3	22	EC	A3	57	F9	39	81	C5
9	5B	FC	B7	C6	F6	A9	0B	C7	CE	33	4C	07	36	2B	A5	23
A	F7	51	E8	60	ED	C2	13	69	3A	C4	55	F2	35	01	CB	25
B	3C	27	D4	59	58	80	04	50	75	70	2F	EE	8F	82	94	09
C	D0	37	F0	E9	D9	EA	9C	8B	9F	63	53	F8	99	0E	65	91
D	A2	0C	61	D2	98	79	02	A4	93	B2	10	28	E0	DD	41	12
E	E6	F4	D5	71	B1	F1	C1	C8	18	5A	BC	49	56	14	BB	42
F	7A	E2	3E	64	B4	29	0A	84	5C	32	52	90	19	21	24	00

. (11)

Шаг 1. Выберем произвольно невырожденную матрицу аффинного преобразования A, например

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{12}$$

Зафиксируем первые 7 её строк, а восьмая строка пусть пробегает все $2^8 = 256$ возможных значений. Найдем все такие структуры восьмой строки, при которых вес производной $wt\left(D_{8,\nu}\right) \geq 128$. Найденные 9 структур восьмой строки поместим в множество Λ, в шестнадцатеричной системе счисления

$$\Lambda = \{17,5C,71,7A,9E,A7,C5,E9,FF\}_h \ . \qquad (13)$$

Построение такой матрицы аффинного преобразования A, которая бы позволяла S-блоку подстановки (11) соответствовать критерию максимального лавинного эффекта возможно тогда, и только тогда, когда объем $|\Lambda| \geq k$, что является необходимым условием.

Шаг 2. На основании данных множества (13) построим $C_9^8 = 9$ квадратных матриц размера (8×8), из которых отберем 5 уникальных конструкций аффинного преобразования, позволяющих получить 5 уникальных S-блоков подстановки, удовлетворяющих критерию максимального лавинного эффекта. Например, рассмотрим одну из матриц $A = [5C,71,7A,9E,A7,C5,E9,FF]^T$, которая в двоичном виде представляется как

$$A = \begin{bmatrix} 0&0&1&1&1&0&1&0 \\ 1&0&0&0&1&1&1&0 \\ 0&1&0&1&1&1&1&0 \\ 0&1&1&1&1&0&0&1 \\ 1&1&1&0&0&1&0&1 \\ 1&0&1&0&0&0&1&1 \\ 1&0&0&1&0&1&1&1 \\ 1&1&1&1&1&1&1&1 \end{bmatrix}. \qquad (14)$$

Применив данное преобразование (14) к S-блоку подстановки (11) получаем новый S-блок подстановки

S	0	1	2	3	4	5	6	7	8	9	*A*	*B*	*C*	*D*	*E*	*F*
0	5C	6A	0D	89	34	D3	DD	E4	47	EA	A4	71	86	87	D9	F9
1	49	7D	92	E6	BB	30	67	8D	DE	05	C4	22	D0	1F	FD	3E
2	72	84	35	56	B5	27	CF	7E	C0	1D	10	61	1A	AA	EE	A7
3	E0	9B	1E	14	E3	F3	70	94	9E	45	25	3C	9F	50	58	C2
4	17	E5	B7	A9	5E	62	28	59	A8	2B	78	B3	F1	C7	2C	44
5	AE	07	33	AD	09	7F	0B	82	73	26	A2	CD	C6	A0	95	EB
6	FC	3B	FA	0F	43	60	6B	4E	D1	A1	AB	E7	20	D6	FB	2E
7	99	F0	5D	96	6E	80	5A	69	DF	CA	52	4B	6C	B6	8C	2A
8	38	DC	8A	D4	C1	2F	AC	FE	4A	BD	40	BF	79	66	0A	54
9	CB	32	76	3A	63	11	A3	C8	F7	37	93	D7	7C	75	65	B8
A	91	9A	04	31	4F	83	E1	0E	08	A6	23	DA	12	F2	BC	9D
B	2D	01	29	57	A5	F8	B9	68	F5	BE	CC	21	E2	64	CE	3F
C	90	8E	46	F6	AF	98	03	5B	6D	5F	06	8B	48	E8	7A	85
D	B2	74	C3	0C	BA	81	9C	97	19	3D	8F	1B	C9	16	15	13
E	EC	FF	DB	4C	53	B4	ED	D2	42	39	D5	D8	4D	36	02	7B
F	EF	55	B1	88	18	E9	51	41	1C	C5	F4	77	B0	24	6F	00

, (15)

удовлетворяющий критерию максимального лавинного эффекта, как это видно из анализа его матрицы весов производных

e_j	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$	$wt\left(D_{7,k}\right)$	$wt\left(D_{8,k}\right)$
10000000	144	136	132	132	140	136	144	128
01000000	128	128	128	140	136	128	132	128
00100000	148	144	132	140	144	136	132	128
00010000	140	128	140	136	132	128	128	128
00001000	136	148	140	144	132	144	132	128
00000100	128	140	136	132	128	128	140	128
00000010	136	136	144	132	132	148	140	128
00000001	128	128	132	128	140	140	136	128

. (16)

Отметим, что различные структуры S-блоков подстановки на основе клеточных автоматов, обладающие простой реализацией и высоким уровнем криптографического качества возможно получить используя различное количество шагов дискретного времени t.

В заключении отметим основные результаты проведенных исследований:

— получила дальнейшее развитие теория синтеза экономичных S-блоков подстановки, в рамках чего предложен эффективный алгоритм синтеза биективных S-блоков подстановки на основе клеточных автоматов, обладающих простой аппаратной и программной реализацией;

— предложена схема улучшения криптографического качества экономичных S-блоков подстановки на основе клеточных автоматов, содержащая дополнительно Z-блок циклического сдвига и A-блок аффинного преобразования;

— установлены правила клеточных автоматов (табл. 2), позволяющие синтез экономичных S-блоков подстановки, отвечающих критерию максимального лавинного эффекта, что является очень важным для противостояния атакам дифференциального криптоанализа;

— полученный выигрыш числа ячеек памяти для однобайтных S-блоков подстановки на основе клеточных автоматов достигает $\gamma_1 = 256 \cdot 8 \big/ 8 = 256$ раз при окрестности $r = 1$, и $\gamma_2 = 256 \cdot 8 \big/ 32 = 64$ раз при окрестности $r = 2$.

Таким образом, клеточные автоматы являются перспективными с криптографической точки зрения конструкциями, позволяющими синтезировать высококачественные и экономичные S-блоки подстановки, которые могут быть рекомендованы к применению в современных криптоалгоритмах.

Литература

1. Nyberg, K. Differentially uniform mappings for cryptography. I Advances in cryptology / K. Nyberg // Proceedings of EUROCRYPT’93 (1994) vol.765, Lecture Notes in Compuer Springer-Verlag, Berlin, Heidelberg, New York. P.55-65.

2. Kim, K. A recursive construction method of S-boxes satisfying strict avalanche criterion / K. Kim, T. Matsumoto, H. Imai // Proc. of CRYPTO’90, Springer — Verlag. — 1990. — P.565—574

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

4. Логачев, О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. — М: Издательство МЦНМО. — 2004. — 472 с.

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

6. Canright, D. A Very Compact S-Box for AES / D. Canright // LNCS 3659, Workshop on Cryptographic Hardware and Embedded Systems (CHES2005). — USA NY: Springer-Verlag. — P. 441-455. — 2005. — ISSN: 0302-9743.

7. Szaban, M. Cryptographically Strong S-Boxes Based on Cellular Automata / M. Szaban, F. Seredynski. — Polnad, Krakow: Lecture Notes in Computer Science, 2008. — Vol. 5191, P. 478—485.

8. Соколов, А.В. Новые методы синтеза нелинейных преобразований современных шифров / А.В. Соколов. — Lap Lambert Academic Publishing, 2015. — 100 с.

9. Ростовцев, А.Г. Криптография и защита информации / А.Г. Ростовцев. — СПб.: Мир и Семья. — 2002.

10. Зайко, Ю.Н. Криптография глазами физика // Изв. Саратовского ун-та. — т. 9 вып. 2. — С. 34—48. — 2009.

11. Chandrasekharappa, T.G.S S-boxes generated using Affine Transformation giving Maximum Avalanche Effect / T.G.S. Chandrasekharappa, K.V. Prema, Kumara Shama // Internation Journal of Computer Science and Engineering. — Manipal Institute of Technology, India. — Vol.3(#9). — 2011. — P.3185—3193.