**Министерство образования и науки,
молодежи и спорта Украины**

ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
РАДИОЭЛЕКТРОНИКИ

МАТЕРИАЛЫ 16-го МЕЖДУНАРОДНОГО МОЛОДЕЖНОГО ФОРУМА

«РАДИОЭЛЕКТРОНИКА И МОЛОДЕЖЬ В XXI веке»

17 – 19 апреля 2012 г.

Том 3

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ «СОВРЕМЕННЫЕ ПРОБЛЕМЫ РАДИОТЕХНИКИ»

Харьков 2012

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА ЭКОНОМИЧНЫХ S-БЛОКОВ НА ОСНОВЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЕ БРЁЙНА

Соколов А.В.
Научный руководитель – д.т.н., проф. Мазурков М.И.
Одесский национальный политехнический университет
(65044, Одесса, пр. Шевченка, 1, каф. информационной безопасности,
тел. (048) 734-84-50), e-mail: radiosquid@gmail.com

Abstract. In this paper we propose a fundamentally new method of modern block ciphers S-boxes forming, which allows to obtain significant reduction in the required memory size for the implementation of the cipher. The investigation of cryptographic properties of the obtained compact S-boxes showed that they have at least equivalent cryptographic quality compare to full-sized ones.

Важнейшим элементом современных блочных шифров, определяющим их криптографическую устойчивость, является блок подстановок (S–блок), структуру которого можно полностью определить кодирующей Q–последовательностью. В настоящее время особый интерес представляет разработка Q–последовательностей, позволяющих добиться снижения требуемой для хранения S–блоков памяти, что существенно увеличивает возможности распараллеливания и конвейеризации шифрования, упрощает требования к аппаратному обеспечению реализации шифра, например, для SMART-карт, а также открывает перспективы к наращиванию криптографической стойкости алгоритмов блочного шифрования в целом. Существующие методы построения экономичных S–блоков позволяют уменьшить объем памяти, требуемой для хранения S–блока на 20% и, зачастую, приводят к существенному снижению криптографических показателей надежности [1].

В настоящей работе предложен метод построения экономичных блоков подстановки, позволяющих уменьшить объем необходимой для хранения S–блока памяти до 4-х раз при сохранении высоких или даже улучшении показателей криптографической устойчивости. Сущность метода заключается в применении в качестве кодирующих последовательностей де Брёйна — циклических k–ичных последовательностей периода k^n со свойством, что каждый k–ичный картеж длины n встречается точно один раз на цикле, например, $Mg = \{15\ \ 14\ \ 13\ \ 11\ \ 6\ \ 12\ \ 9\ \ 2\ \ 5\ \ 10\ \ 4\ \ 8\ \ 0\ \ 1\ \ 3\ \ 7\}$. Данные псевдослучайные последовательности обладают такими важными для блоков подстановок качествами как сбалансированность и высокая непредсказуемость. В рамках проводимого исследования были разработаны методики построения блоков подстановок на основе двоичных и четверичных последовательностей де Брёйна и изучены их криптографические свойства по базовым критериям, обоснованным в [2, 3]:

1. Отсутствие корреляционной связи между входными и выходными битами S–блока. Для оценки данного критерия потребуем равномерность рас-

пределения элементов матрицы коэффициентов корреляции $|r_{\max}| \le 1/\eta$, где η – размерность компонентной функции S–блока.

2. Максимальное расстояние нелинейности, которое для сбалансированных функций не превышает значения $d_{S\max} \le 2^{\eta-1} - 2^{(\eta/2)-1} - 2$.

3. Максимальная длина циклов, на которые раскладывается подстановка, определяемая как $T = HOK(i_1, i_2 ...)$, где i – соответствующие длины циклов.

4. Строгий лавинный критерий, определяемый через коэффициент распространения ошибки как $K_i(f) = \sum_{e_i} (f(x) \oplus f(x \oplus e_i)) = 2^{\eta-1}$.

Приведем таблицу, иллюстрирующую значение вышеуказанных показателей криптографической стойкости для различных классов последовательностей де Брёйна.

Таблица – Значения криптографически важных показателей S–блоков

Класс последовательностей де Брёйна	Объем класса $W = 2^{N/2}$	Количество J S–блоков, обладающих заданным параметром				Экономия памяти, раз
		$\lvert r_{\max}\rvert \le 1/\eta$	$d_S = 2^{\eta-1} - 2^{\frac{\eta}{2}-1} - 2$	T	$K_i(f) = 2^{\eta-1}$	
двоичн., $n = 4$	256	24	192	21 ($T \ge 60$)	0	4
двоичн., $n = 5$	65536	76	33032	1642 ($T \ge 1000$)	0	4
четверичн., $n = 2$	331776	23008	218688	2281 ($T = 140$)	2176	2

Таким образом, применение последовательностей де Брёйна для построения экономичных блоков подстановок позволяет достичь многократного снижения объема требуемой для реализации алгоритма памяти, при сохранении оптимальных криптографических и перемешивающих свойств. Применение четверичных последовательностей де Брейна, позволяет получить существенное увеличение числа доступных экономичных S–блоков за счет некоторого снижения уровня экономии памяти, что обеспечивает гибкость применения последовательностей де Брёйна при выборе параметров блока подстановок для конкретной практической задачи.

Список источников: 1. 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, pp. 441-455.– 2005. – ISSN: 0302-9743. 2. Долгов В.И. Подстановочные конструкции современных симметричных блочных шифров./ Долгов В.И., Олейников Р.В., Лисицкая И.В., Сергиенко Р.В., Дроботько Е.В. Мельничук Е.Д. // Радіоелектронні і компютерні системи, ХНУРЭ, – 2009, – №6.– С.89-93. 3 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.