УДК 621. 391:519.2:519.7

СНОВА ОБ ОПТИМАЛЬНЫХ S-БЛОКАХ

К.Е. ЛИСИЦКИЙ

Приводятся результаты оценки динамических показателей процесса прихода шифра Хейза и уменьшенной модели шифра Rijndael по дифференциальным показателям к стационарным состояниям, свойственным случайным подстановкам при использовании в шифрах полубайтовых подстановок, сконструированных различными способами. Показано, что предлагаемый в одной из последних публикаций метод формирования оптимальных Q-S-блоков с использованием квазигрупп на самом деле не приводит к подстановкам с улучшенными криптографическими показателями. Делается вывод, что поиск полубайтовых S-блоков с улучшенными свойствами потерял смысл. Лучшие подстановочные преобразования уже получены на основе полного перебора всего множества полубайтовых подстановок симметрической группы.

Ключевые слова: подстановка, оптимальный S-блок, динамические показатели шифра, максимумы полных дифференциалов.

ВВЕДЕНИЕ

В научных публикациях уже поднимался вопрос о не перспективности направления, интенсивно развиваемого в криптографии, связанного с разработкой математических методов конструирования S-блоков с улучшенными криптографическими показателями, которые, как правило, ищут среди подстановок с минимально возможными значениями дифференциальных и линейных вероятностей. Этот вывод основывается на многочисленных экспериментах с уменьшенными моделями большого числа современных шифров. Результаты экспериментов свидетельствуют о том, что показатели стойкости шифров к атакам дифференциального и линейного криптоанализа от свойств используемых S-блоков практически не зависят [1] (за исключением шифра DES и близких к нему, допускающих использование при построении дифференциальных характеристик цикловых переходов обнуляющего типа).

Если говорить об эффективности подстановочного преобразования, то она определяется совместно с шифрующим преобразованием с помощью динамических показателей, в качестве которых выступают оценки числа циклов шифра, необходимых ему для перехода к стационарному состоянию, свойственному случайной подстановке соответствующей степени [2]. Речь идёт о числе циклов зашифрования, после которого законы распределения переходов таблиц XOR разностей и смещений таблиц линейных аппроксимаций шифра начинают повторять соответствующие законы распределения вероятностей случайных подстановок. И здесь оказывается, что во многих случаях S-блоки и не с минимальными значениями вероятностей дифференциальных и линейных характеристик обеспечивают наилучшие динамические свойства. В частности, в [1] показано, что в качестве S-блоков практически всех современных шифров могут выступать подстановки случайного типа. Именно процесс прихода к стационарному состоянию, характеризуемый числом циклов шифрования, является объективным свидетельством качества шифрующего преобразования в целом, а, следовательно, и используемых в шифре подстановочных преобразований.

Недавно появилась ещё одна публикация [3], в которой авторы претендуют на создание новой методики конструирования полубайтовых S-блоков с улучшенными криптографическими свойствами. В противовес работе [4], в которой «идеальные» S-блоки получены путём полного перебора всего множества полубайтовых подстановок, они претендуют на создание математического аппарата получения S-блоков с предельными, как они считают, криптографическими показателями.

В этой работе воспользуемся ещё одной возможностью продемонстрировать, во-первых, – далеко не лучшие свойства предлагаемых в [3] конструкций S-блоков в отношении реализации оптимальной динамики шифрующих преобразований, в которых они участвуют, а во-вторых, – ещё раз заострить внимание на том, что для полубайтовых подстановок вопрос с построением оптимальных конструкций уже полностью решён.

В первой части статьи приводится краткая характеристика предлагаемого в работе [3] метода и выделяются результативные её моменты. Во второй части излагаются результаты статистических экспериментов по оценке динамических свойств шифра Хейза со слабым линейным преобразованием и шифра Rijndael с сильным линейным преобразованием при использовании в этих шифрах подстановок различных конструкций, в том числе и подстановок, полученных с помощью предлагаемого в работе [3] метода.

1. КРАТКАЯ ХАРАКТЕРИСТИКА РЕЗУЛЬТАТОВ РАБОТЫ [3]

В своей работе авторы сосредотачиваются на так называемой легковесной (lightweight) симметричной криптографии. Несмотря на то, что блочный шифр AES (Advanced Encryption

Standard) является одним из наиболее используемых криптографических примитивов, он в основном предназначен для эффективной программной реализации. Для многих ограниченных сред (применений), использование AES в качестве блочного шифра является либо слишком дорогим, либо нет необходимости для такого высокого уровня безопасности, который предлагает этот шифр. Поэтому, не удивительно, что в последние несколько лет наблюдается динамичное развитие в области легковесной криптографии, особенно в области легких блочных шифров, таких как PRESENT [4–5].

Основой безопасности в симметричной криптографии, почти во всех современных блочных шифрах, являются подстановки, известные также как S-блоки. S-блоки работают с небольшим набором данных, поэтому они должны отличаться высокими нелинейными свойствами, если хотят, чтобы они запутывали входные данные в шифре. PRESENT является ультра-легким блочным шифром, предложенным Богдановым и др. [2]. Отмечается, что он был разработан для чрезвычайных условий в виде весьма ограниченных ресурсов, таких как метки RFID (англ. Radio Frequency IDentification). Приводится краткое описание шифра. PRESENT является SPN блочным шифром, который состоит из 31 цикла и работает на 64-битных блоках данных. Он поддерживает две длины ключа 80 или 128 бит, где 80-битный ключ рекомендуется к использованию. Каждый из 31 циклов выполняется за три этапа (слоя). На первом этапе осуществляется сложение блока данных с цикловым подключом – AddRoundKey, второй этап – слой подстановок – SBoxLayer, и третий этап является битовой перестановкой pLayer. Наиболее интересным является второй этап, где главная роль принадлежит S-блокам. В нелинейном слое (SBoxLayer) используются одинаковые 4×4-битные S-блоки. Выбор 4×4-битных S-блоков является прямым следствием преследования авторами цели повышения эффективности применяемого оборудования, где реализация таких S-блоков, как правило, является гораздо более компактной и требует меньше ресурсов, чем 8×8-битные S-блоки. 4-битные S-блоки требуют менее четверти аппаратных затрат по сравнению с 8-битными S-блоками.

С точки зрения криптографии, 4-битные S-блоки должны выбираться очень тщательно, потому что они слабее, чем 8-битные S-блоки.

Далее отмечается, что S-блоки шифра PRESENT получены в результате перебора всех 16! биективных 4-битных S-блоков. Все S-блоки, найдены таким образом, что были выполнены дополнительные критерии оптимальности, и чтобы они были проанализированы с точки зрения линейной эквивалентности. Так, существует только 16 различных неэквивалентных классов [6]. Все S-блоки, члены в этих классах, являются оптимальными S-блоками в отношении линейных и дифференциальных свойств. Эти S-блоки также оптимальны по отношению к алгебраической степени или сопротивляемости к алгебраическим атакам.

Заметим, что аналогичная работа по поиску оптимальных подстановок прямым перебором всего множества полубайтовых S-блоков выполнена в работе [7]. В ней получены S-блоки, названные золотыми. Им посвящена работа [8].

Вместо перебора всех 16! биекций из 16 элементов, как это было сделано при проектировании до настоящего времени, предлагается компактная, быстрая и элегантная методология построения криптографически сильных S-блоков с помощью квазигрупп порядка 4. Целью, которую поставили перед собой авторы работы, является дать криптографам итерационный инструмент для проектирования криптостойких S-блоков, которые обозначены ими как QS-блоки, поскольку их строительство осуществляется с помощью квазигрупп. В общем, предлагаются S-блоки, которые, являются конкурентоспособными S-блоку шифра PRESENT.

Мы не будем здесь детально останавливаться на развиваемой в работе методологии, а остановимся сразу на её результатах.

В работе [3] приведено три примера «оптимальных Q-S-блоков, построенных по предлагаемому методу. Первый Q-S-блок представляет результаты применения методики (в обозначении авторов работы) с двумя лидерами и четырьмя циклами. Отмечается, что всего число таких Q-S-блоков, у которых выходные биты имеют алгебраическую степень 3, есть 128. Один из них представлен в работе, и он же приведен в третьей строке табл. 1. Авторы в [3] приводят ещё два примера построения Q-S-блоков, они также помещены в табл. 1 (строки первая и вторая).

В четвёртой строке табл. 1 представлен один из Q-S-блоков, построенных с помощью методики с четырьмя лидерами и четырьмя циклами (один лидер в каждом цикле). Число Q-S-боксов, у которых все выходные биты имеют алгебраическую степень 3, в данном случае равно 1024.

В пятой строке таблицы представлен пример ещё одного из Q-S-блоков для эксперимента с восемью лидерами и восемью циклами. Число QS-блоков, у которых все выходные биты здесь имеют алгебраическую степень 3, равно 331264.

В седьмой строке таблицы представлен S-блок шифра PRESENT, в девятой–двенадцатой строках приведены примеры золотых S-блоков из работы [7], а в двух последних строках приведены S-блок шифра DES (первая строка первого S-блока) и S-блок шифра AES (полубайтовый S-блок, построенный по идеям разработчиков шифра).

Заострим попутно внимание на формальном определении оптимального S-блока, приведенном в работе [3].

Таблица 1

Примеры S-блоков, участвующих в экспериментах

S-блоки из работы [3]																
Нулевая строка	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S_1(x)$	C	1	2	E	F	9	3	4	8	0	A	B	7	D	6	5
$S_2(x)$	D	9	F	C	B	5	7	6	3	8	E	2	0	1	4	A
$S_3(x)$	5	E	6	D	7	4	2	A	8	C	0	9	1	B	F	3
S-блок шифра PRESENT																
$S_4(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
«Золотые» S-блоки из работы [7]																
$S_5(x)$	0	3	5	8	6	9	C	7	B	A	E	4	1	F	B	2
$S_6(x)$	0	3	5	8	6	A	F	4	E	D	9	2	1	7	C	B
$S_7(x)$	0	3	5	8	6	C	B	7	9	E	A	D	F	2	1	4
$S_8(x)$	0	3	5	8	6	C	B	7	A	4	9	E	F	1	2	D
S-блоки шифров DES и AES																
$S_9(x)$	A	4	3	B	8	E	2	C	5	7	6	F	0	1	9	D
$S_{10}(x)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Определение. Пусть S будет 4×4-битным S-блоком. Если S полностью удовлетворяет приведенным ниже условиям, мы называем S оптимальным S-блоком:

S является биекцией;

Lin(S) = 1/4 (максимальное значение вероятности линейной аппроксимационной таблицы S-блока);

Diff(S) = 1/4 (максимальное значение вероятности перехода XOR таблицы S-блока).

Все Q-S-блоки табл. 1 являются оптимальными в отмеченном смысле.

После этих кратких сведений можно приступить уже к анализу результатов выполненных оценок дифференциальных свойств шифров, использующих различные конструкции S-блоков.

2. РЕЗУЛЬТАТЫ СТАТИСТИЧЕСКИХ ЭКСПЕРИМЕНТОВ С УМЕНЬШЕННЫМИ МОДЕЛЯМИ ШИФРОВ С РАЗЛИЧНЫМИ КОНСТРУКЦИЯМИ ПОДСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ

В табл. 2 приведены результаты оценки дифференциальных показателей шифра Хейза [9] с различными S-блоками. В первой колонке приведены данные о применении в шифре идеального S-блока из работы [7] (9-я строка табл. 1), во второй, третьей и четвёртой колонках представлены дифференциальные показатели (поцикловые значения максимумов полных дифференциалов) шифра Хейза, когда в нём используются S-блоки из рассматриваемой работы [3] (3–5 строки табл. 1). В остальных колонках табл. 2 в шифре используются S-блоки из шифров DES (первая строка первого S-блока) и AES («родной» S-блок) и, наконец, S-блок шифра PRESENT (7-я строка табл. 1). Во всех случаях в шифре применялись наборы из одних и тех же S-блоков.

Из представленных результатов следует, что предлагаемая в работе [3] методика позволяет получить S-блоки, отнюдь не обладающие оптимальными динамическими свойствами. Число циклов для прихода к стационарному состоянию, характерному для случайной подстановки, для всех трёх примеров оказалось превышающем семь. S-блок $S_1(x)$ выходит к асимптотическому значению лишь на одиннадцатом цикле. Такие показатели свойственны случайным S-блокам [2].

Рассматриваемые S-блоки оказались ничуть не лучше уже известных S-блоков, заметно усту-

Таблица 2

Значения максимумов полных дифференциалов для различных S-блоков и различного количества циклов алгоритма Хейза

Sbox *r*	Идеальный Sbox	S-box S_1	S-box S_2	S-box S_3	S-box DES	S-box AES	S-box PRESENT
1	16384	16384	16384	16384,00	32768,00	16384,00	16384,00
2	4096	4096	4096	4096,00	12288,00	4096,00	4096,00
3	512,13	2048,00	2338,67	1454,93	2303,33	2036,27	516,27
4	81,40	1132,00	631,47	404,40	222,27	596,00	61,07
5	30,40	514,07	278.00	119,53	64,13	190,33	24,93
6	**19,20**	229,47	113,40	43,67	24,80	77,47	**18,93**
7	19,07	116,93	51,53	20,60	**18,80**	35,87	19,40
8	19,87	59,87	27.40	**19,13**	18,80	21,07	18,80
9	19,07	32,13	**19,07**	19,07	19,00	**19,27**	19,27
10	19,53	20,47	19,20	19,13	18,93	19,33	19,13
11	19,13	**18,73**	18,47	19,20	18,93	19,00	18,93

пая по динамическим показателям идеальным S-блокам из работы [6]. Осталось засомневаться в качестве S-блоков, использованных в шифре PRESENT. Но как показывают результаты экспериментов (см. последнюю колонку табл. 2), в шифре PRESENT S-блоки, выбранные путём полного перебора, повторяют характеристики идеальных S-блоков из работы [7] (также полученных путем полного перебора всех 16! полубайтовых подстановок симметрической группы).

В табл. 3 приведены результаты экспериментов с уменьшенной моделью шифра Rijndael, в котором опять использованы S-блоки из табл. 2. Здесь шифр Rijndael выступает как шифр с сильным линейным преобразованием, в противовес щифру Хейза, который в наших экспериментах отражал шифр со слабым линейным преобразованием.

Из полученных результатов следует, что шифр с сильным линейным преобразованием не чувствует разницы между S-блоками. Для него все S-блоки оказались эквивалентными по динамическим показателям прихода шифра к стационарному состоянию. Предлагаемые конструкции S-блоков здесь никаких преимуществ по сравнению с другими не имеют, и S-блоки, не являющиеся в рассмотренном выше смысле оптимальными, показывают высокие результаты.

Учитывая дуальную связь дифференциальных и линейных показателей, можно сделать вывод, что аналогичные результаты будут справедливы и для линейных корпусов рассмотренных шифров (линейные и дифференциальные показатели по динамике близки друг к другу [10 и др.]).

ВЫВОДЫ

Представленные результаты экспериментов свидетельствуют, что предлагаемый в работе метод получения оптимальных S-блоков не может претендовать на оригинальность и полезность. Криптографические показатели формируемых S-блоков значительно уступают золотым (идеальным) S-блокам из работы [6] и показателям S-блоков шифра PRESENT [2]. Они практически повторяют динамические показатели S-блоков, сгенерированных случайным образом.

Для шифров с сильным линейным преобразованием поиск S-блоков с улучшенными криптографическими показателями теряет смысл. Здесь задача может быть успешно решена на основании использования S-блоков, сгенерированных случайным образом.

С другой стороны, раз оказываются востребованными шифры со слабыми линейными преобразованиями, то задача поиска оптимальных полубайтовых S-блоков для них практически решена. В качестве таких решений могут выступать идеальные (золотые) S-блоки, найденные в работе [6]. Они с успехом применяются уже в шифрах Serpent и PRESENT. И в этом случае задача поиска оптимальных S-блоков также теряет смысл.

Нельзя не отметить ещё один важный полученный результат. Он состоит в том, что шифр PRESENT со своими S-блоками имеет весьма высокий запас прочности. Он с успехом сможет реализовать потенциальные показатели по стойкости к атакам дифференциального и линейного криптоанализа и при числе циклов зашифрования более чем вдвое меньшем заявленного в разработке, если учитывать и сопротивляемость шифра к бумеранг атаке, требующей от шифра обеспечения стойкости на половине его цикловой длины.

Литература

[1] *Lisitskaya I.V.* Importance of S-Blocks in Modern Block Ciphers. / I.V. Lisitskaya, E.D. Melnichuk and K.E. Lysytskiy. // I.J. Computer Network and Information Security – 2012. – 10 – С. 1–12.

[2] *Лисицкая И.В.* Методология оценки стойкости блочных симметричных шифров. / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123–133.

[3] *Hristina Mihajloska*, Skopje, Macedonia, Danilo Gligoroski Construction of Optimal 4-bit S-boxes by Quasigroups of Order 4 SECURWARE 2012 : The Sixth International Conference on Emerging Security Information, Systems and Technologies pp. 163–168.

[4] *A. Bogdanov, L. R. Knudsen, G. Le, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe,* "PRESENT: An Ultra-Lightweight Block Cipher," in The Proceedings of CHES 2007. Springer-Verlag, 2007. – P. 450–466.

[5] *T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel,* "A Survey of Lightweight-Cryptography Implementations," in IEEE Design and Test, vol. 24, no. 6. IEEE Computer Society Press, November, 2007. – P. 522–533.

[6] *G. Leander and A. Poschmann,* "On the Classification of 4 Bit S-Boxes," in Proceedings of the 1st International Workshop on Arithmetic of Finite Fields. Springer-Verlag, 2007. – P. 159–176.

Таблица 3

Значения максимумов полных дифференциалов для различных S-блоков и количества циклов алгоритма Rijndael. Линейная часть – MixColumn GF(2^4) и ShiftRow.

S-box r	S-box идеальный	S-box S_1	S-box S_2	S-box S_3	S-box PRESENT	S-box DES	S-box AES	Случайный S-box
1	16384	16384,00	16384,00	16384,00	16384,00	32768,00	16384,00	49152,00
2	3054,93	3413,33	3106,13	3037,87	3089,07	1152,00	3072,00	5184,00
3	381,60	353,07	290,13	340,27	314,67	70,87	272,00	146,13
4	19,53	19,53	19,40	19,33	19,33	19,27	19,20	19,07
5	18,93	19,20	19,13	19,13	19,20	19,00	19,27	19,00
6	19,07	19,07	19,13	19,20	18,47	19,00	19,13	19,00

[7] *Markku-Juhani O. Saarinen*: Cryptographic Analysis of All 4 x 4 - Bit S-Boxes, In SAC 2011, August 2011 Toronto, Canada, Springer LNCS. A version is available at eprint.iacr.org/2011/218/

[8] *Кобылина Ю.И.* Дифференциальные свойства малых версий современных шифров при использовании в них идеальных подстановок / Ю.И. Кобылина, К.Е. Лисицкий // Сборник трудов Второй Международной научно-технической конференции «Компьютерные науки и технологии» 3-5 октября. – Белгород. – 2011. – С. 423–425.

[9] *H. M. Heys.* A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v 26, N 3, 2002. – P. 189–221.

[10] *Лисицька І.В.* Большие шифры – случайные подстановки. Сравнение дифференциальных и линейных свойств шифров, представленных на украинский конкурс и их уменьшенных моделей / І.В. Лисицька, А.А. Настенко, К.Є. Лисицький // Автоматизовані системи управління та прибори автоматики. – 2012. – Т. 159. №. – С. 31–39.

Поступила в редколлегию 27.06.2014

Лисицкий Константин Евгеньевич, магистр Харьковского национального университета им. В.Н. Каразина. Научные интересы: технологии блочного симметричного шифрования.

УДК 621. 391:519.2:519.7

Знову про оптимальні S-блоки / К.Є. Лисицький // Прикладна радіоелектроніка: наук.-техн. журнал. — 2014. — Том 13. — № 3. — С. 208–212.

Наводяться результати оцінки динамічних показників процесу приходу шифру Хейза і зменшеної моделі шифру Rijndael за диференціальними показниками до стаціонарних станів, властивих випадковим підстановкам в ході використання в шифрах напівбайтових підстановок, сконструйованих різними способами. Показано, що запропонований в одній з останніх публікацій метод формування оптимальних QS-блоків з використанням квазігруп насправді не призводить до підстановок з поліпшеними криптографічними показниками. Робиться висновок, що пошук напівбайтових S-блоків з поліпшеними властивостями втратив сенс. Кращі підстановлювальні перетворення вже отримано на основі повного перебору всієї множини напівбайтових підстановок симетричної групи.

Ключові слова: підстановка, оптимальний S-блок, динамічні показники шифру, максимуми повних диференціалів.

Табл.: 3. Бібліогр.: 10 найм.

UDC 621. 391: 519. 2: 519.7

Again on optimum S-boxes / K.E. Lisitsky // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 208–212.

The paper presents the results of evaluating the dynamic performance of the Heys cipher coming process and cipher Rijndael reduced model by differential performance to steady states typical of random substitutions in using ciphers nibble substitutions engineered in various ways. It is shown that the method of forming optimum QS-blocks with the use of quasi-groups, which was suggested in one of recent publications, do not actually lead to substitutions with improved cryptographic parameters. A conclusion is drawn that searching nibble S-units with improved properties has become pointless. The best wildcard transformations have already been obtained on the basis of an complete exhaustion of the whole set of nibble substitutions of a symmetric group.

Keywords: substitution, optimal S-box, dynamic cipher performance, maxima of total differentials.

Tab.: 3. Ref.: 10 items.