УДК 621. 3.06

В.И. ДОЛГОВ, д-р техн. наук, Е.В. МЕЛЬНИЧУК

S-БЛОКИ ДЛЯ СОВРЕМЕННЫХ ШИФРОВ

Введение

В предыдущей работе [1] было показано, что S-блоки для блочных симметричных шифров с хорошими криптографическими показателями можно выбрать на основе случайного отбора. Для байтовых S-блоков это сделать совершенно просто, так как с высокой вероятностью случайно выбранный S-блок будет обладать криптографическими свойствами, не уступающими лучшим известным конструкциям S-блоков. Здесь имеется в виду новый показатель оценки эффективности S-блоковых конструкций введенный в работе [1], который строится на основе оценки числа циклов шифра, необходимых ему для прихода к стационарному состоянию, свойственному случайной подстановке. Более совершенными будут считаться те S-блоки, с которыми шифр приходит к стационарным значениям максимумов полных дифференциалов и максимумов смещений линейных оболочек, характерных для случайной подстановки, за меньшее число циклов

В данной статье ставится задача подтвердить это положение на примере отбора подстановок (случайных S-блоков) для известного мирового лидера – шифра Rijndael и шифров, представленных на прошедший украинский конкурс по выбору претендента на национальный стандарт шифрования.

Методика выполнения исследований

Методика определения дифференциальных и линейных показателей полноразмерных шифров подробно представлена в работах [2, 3 и др.]. Основой этой методики является определение поцикловых значений максимумов 16-битных разностей (полных дифференциалов) и 16-битных значений максимумов смещений линейных оболочек для сегментов блоков данных на входах и выходах шифров с разными конструкциями S-блоков с последующим сравнением между собой этих решений по числу циклов, необходимых для прихода каждого из шифров к показателям случайной подстановки, т.е. практически строятся существенно уменьшенные части таблиц полных дифференциалов и смещений таблиц линейных аппроксимаций больших шифров, и на основе сравнительной оценки показателей этих усеченных таблиц принимается решение о преимуществах того или иного варианта построения шифра, а значит, и S-блоков, использованных в нем.

S-блоки для шифра Rijndael

Далее излагаются результаты вычислительных экспериментов. В табл. 1 представляются поцикловые значения максимумов полных дифференциалов для шифра Rijndael с различными S-блоками. В первой колонке приведены данные для шифра Rijndael с использованием стандартных S-блоков. В колонках под номерами 2 − 6 в шифре Rijndael используются случайно порожденные S-блоки, причем при отборе случайных S-блоков на них не накладывались никакие ограничения. Взяты подряд пять случайно сгенерированных S-блоков.

Как было отмечено, в экспериментах строились дифференциальные таблицы для 16-битных разностей на входе и выходе шифров. Использовались разности для 4-го и 7-го байтов входа и выхода.

В качестве мастер-ключей взяты случайно порожденные 128-битные блоки, приведенные в табл. 2.

Во всех случаях использовалась стандартная схема разворачивания ключа. Общий вывод из представленных результатов состоит в том, что подряд взятые случайные S-блоки обеспечивают для шифров дифференциальные показатели, практически не уступающие показателям шифра с ″родными″ S-блоками, отобранными по специальным условиям. Полу-

чается, что ″охота″ за S-блоками с улучшенными криптографическими показателями, ведущаяся активно в криптографической литературе, не имеет смысла.

Таблица 1

Число циклов	Подстановки					
	1	2	3	4	5	6
1	65536	65536	65536	65536	65536	65536
2	24	18	20	18	20	20
3	20	18	18	20	18	20
4	18	18	18	18	20	18
5	18	18	20	18	18	20
6	20	20	18	22	18	20
7	18	20	20	20	18	20
8	20	18	20	20	20	20
9	20	20	20	18	18	20
10	18	18	20	20	20	18
11	18	18	18	18	18	18
12	20	20	20	20	20	20
13	18	18	20	20	18	20

Таблица 2

№	Мастер-ключи
1	B7CC40EC614A6410965517B40CDEEB5ADD76369264B5AC3EA16D2FF8DDC15
2	A97F2F19A1115A3833E6C7D3126E8D5A1FA8BCC3A5E963A13818B9E1DFFE45A
3	5F21A0D64CDEC949A41FB7B1EB8C66E2C07BC7F8314C3BBC22D2D403924C2A5
4	C0F3765F31666EF6F86F7B1AD9DECA8926AF75B438A9A8D4C1FB71822CAE1F
5	91E561CDAB2E2A88D53360BDB3BF265333EEB580DCAFCFAC31173488A1557C
6	EF25ACE0553F879F4DF48E14B6AD650A6308253B850C9B5526FC2A506AD

Для более полного отражения криптографических свойств шифров в табл. 3 и 4 представлены поцикловые законы распределения переходов таблиц полных дифференциалов для шифра Rijndael с родной подстановкой (табл. 3) и этого же шифра – со случайной подстановкой 1 (табл.4). Из табл. 3 и 4 хорошо видно, что законы распределения вероятностей, начиная уже с первого цикла, очень близки друг к другу.

В табл. 5 представлены конкретные показатели подстановок S-блоков (одинаковых) шифра Rijndael.

В табл. 6 для сравнения приведены характеристики случайного S-блока под номером 2 в табл. 1 (этот же S-блок приведен под номером 1 в табл.2). Сравнение результатов табл. 5 и 6 показывает, что случайный S-блок по комбинаторным показателям оказывается близким к специально отобранному S-блоку шифра Rijndael, в то время как законы распределения переходов и смещений соответствующих таблиц заметно отличаются друг от друга.

Далее приведены результаты экспериментов с шифром Rijndael, но теперь для него строятся поцикловые распределения максимумов линейных оболочек.

В табл. 7 в первой колонке приведены показатели шифра для стандартной подстановки (табл. 5), а в колонке 2 используется случайно сгенерированный S-блок из табл. 6.

И в этом случае результаты свидетельствуют о том, что шифр Rijndael со случайными S-блоками практически не уступает по эффективности (по числу циклов, необходимых для перехода к показателям случайной подстановки) оригинальной разработке. Для получения 16-битного входа/выхода были взяты 4-й и 7-й байты входного и выходного блоков полноразмерного шифра AES с размером блока 256 бит и длиной ключа 256 бит.

Таблица 3

Число циклов	Rijndael с родной подстановкой. Числа ячеек таблицы полных дифференциалов по их заполнениям												
	0	2	4	6	8	10	12	14	16	18	20	22	512
1	4286545665	0	0	0	0	0	0	0	0	0	0	0	$8{,}3\cdot10^{6}$
2	2604966614	$1{,}30\cdot10^{9}$	325651069	54255750	6775997	679213	56358	4109	262	3	1	0	0
3	2604978428	$1{,}30\cdot10^{9}$	325613734	54269116	6785299	678244	56157	3982	265	21	1	0	0
4	2605010786	$1{,}30\cdot10^{9}$	325648583	54268197	6783670	678427	56728	4125	243	15	0	0	0
5	2604983918	$1{,}30\cdot10^{9}$	325605055	54275819	6784332	678419	56753	4021	234	18	0	0	0
6	2605008408	$1{,}30\cdot10^{9}$	325617103	54280422	6787319	677529	56344	3932	287	20	3	0	0
7	2605000214	$1{,}30\cdot10^{9}$	325623218	54272761	6784787	679016	56636	4159	269	19	0	0	0
8	2604947277	$1{,}30\cdot10^{9}$	325616851	54258309	6782134	677200	56351	4042	226	16	1	0	0
9	2604952924	$1{,}30\cdot10^{9}$	325621156	54255725	6783272	677706	56566	3973	287	14	1	0	0
10	2604968362	$1{,}30\cdot10^{9}$	325629098	54261284	6781522	678581	56346	3926	224	9	0	0	0
11	2604965638	$1{,}30\cdot10^{9}$	325627806	54261335	6783337	676394	56550	4012	247	18	0	0	0
12	2604962347	$1{,}30\cdot10^{9}$	325627417	54258891	6780754	678731	56652	4006	240	11	2	0	0
13	2604987639	$1{,}30\cdot10^{9}$	325617247	54268082	6785738	679260	56582	4035	266	14	0	0	0

Таблица 4

Число циклов	Rijndael с родной подстановкой, 4-й и 7-й байт входа/выхода. Числа ячеек таблицы полных дифференциалов по их заполнениям														
	0	2	4	6	8	10	12	14	16	18	20	22	512	1024	65536
1	4286552577	0	0	0	0	0	0	0	0	0	0	0	$8\cdot10^{6}$	6912	255
2	2605185259	302205809	325640895	54324835	6802164	681450	56881	4169	282	15	1	0	0	0	0
3	2604968650	302524923	325615136	54279227	6776220	676897	56586	3862	243	15	1	0	0	0	0
4	2604914122	302616478	325600024	54254205	6778669	677154	56752	4077	269	10		0	0	0	0
5	2604976365	302521578	325612992	54265532	6785419	678839	56688	4073	256	16	2	0	0	0	0
6	2604993128	302492271	325620412	54270903	6785308	679123	56355	3999	244	16	1	0	0	0	0
7	2604997373	302481170	325628952	54269811	6785059	678762	56371	4009	240	12	1	0	0	0	0
8	2604965272	302523997	325631025	54264889	6778260	677406	56600	4010	285	14	2	0	0	0	0
9	2604998699	302493460	325603183	54279388	6787784	678264	56710	4018	239	14	1	0	0	0	0
10	2604983934	302504978	325619403	54272514	6780828	679031	56728	4047	283	14		0	0	0	0
11	2604978318	302507735	325630814	54263127	6782379	678333	56715	4056	274	9		0	0	0	0
12	2604972063	302524389	325616253	54266366	6783979	677808	56651	3997	243	8	3	0	0	0	0
13	2604965308	302531402	325621514	54262662	6781353	678683	56526	4028	272	11	1	0	0	0	0

.

Таблица 5

Количество циклов: 5 Количество инверсий: 16753 Количество возрастаний: 126
Максимум таблицы XOR: 4 Количество максимумов таблицы XOR: 255 Распределение элементов таблицы XOR 0: 32640 2: 32130 4: 255
Максимум таблицы LAT: 16 Количество максимумов таблицы LAT: 1275 Распределение элементов таблицы LAT 0: 4080 2: 12240 4: 9180 6: 10200 8: 8670 10: 6120 12: 9180 14: 4080 16: 1275

Таблица 6

Количество циклов: 5 Количество инверсий: 16849 Количество возрастаний: 130	
Максимум таблицы XOR: 10 Количество максимумов таблицы XOR: 9 Распределение элементов таблицы XOR	
0: 39277 2: 19865 4: 4998	6: 779 8: 100 10: 9
Максимум таблицы LAT: 34 Количество максимумов таблицы LAT: 1 Распределение элементов таблицы LAT	
0: 6633 2: 12046 4: 11711 6: 9640 8: 8119 10: 5872 12: 4276 14: 2784 16: 1799	18: 1035 20: 575 22: 281 24: 135 26:75 28:30 30: 10 32: 3 34: 1

Таблица 7

Число циклов	Стандартная подстановка	Случайная подстановка
1	11264	10752
2	852	804
3	807	812
4	805	812
5	843	796
6	874	800
7	808	806
8	876	824
9	810	815
10	817	840
11	840	827
12	811	843
13	818	811

Из табл. 7 видно, что законы распределения вероятностей, начиная с первого цикла, очень близки друг к другу.

Рассмотрим теперь, как будут вести себя со случайными S-блоками шифры украинского конкурса. Здесь будем рассматривать три шифра: Калину, Мухомор и Лабиринт [4 – 6]. У шифра ADE в процессе экспертизы были обнаружены слабости [7], поэтому здесь исключим его из рассмотрения.

S-блоки для шифра Калина

В шифре Калина [5] используются восемь разных S-блоков, отобранных по специальным требованиям, о которых в спецификации не сообщается. Результаты тестирования шифра Калина с S-блоками, взятыми из спецификации шифра, представлены в первой колонке табл. 8. В остальных колонках этой таблицы представлены результаты зашифрования шифра Калина с комплектами (наборами) S-блоков, сгенерированных случайным образом. Хорошо видно, что свойства шифра для разных наборов S-блоков получились практически идентичными. Главное, что здесь есть свобода в выборе предпочтительного варианта. Заметим, что нулевое значение максимума дифференциальной таблицы связано с тем, что в экспериментах используется 16-битная разность на основе использования 4-го и 7-го байтов входа и выхода (байты нумеруются, начиная с нуля!). В результате после операции MixColumns первого цикла байты сдвигаются, и на местах 4-го и 7-го байтов выхода оказываются нулевые разности. Если бы формировались разности на основе, например, 0-го и 1-го байтов, то уже после первого цикла получили бы значение максимума дифференциальной таблицы равное $18 - 20$ (сразу бы получили показатель максимума случайной подстановки).

В табл. 8 в первой колонке приведены поцикловые значения максимумов таблиц дифференциальных разностей для восьми стандартных подстановок шифра Калина. Во второй колонке приведены средние значения максимумов для 10 экспериментов с применением 80 случайных подстановок (по восемь на каждый эксперимент). В последней колонке представлены максимумы для первого набора из восьми случайных подстановок.

В табл. 9 по аналогии с шифром Rijndael представлены линейные показатели шифра Калина. И эти результаты свидетельствуют о том, что Калина со случайными S-блоками оказывается вполне конкурентоспособной шифру в авторской разработке.

S-блоки для шифра Мухомор

В шифре Мухомор S-блоки также приведены в спецификации без особых оговорок. В табл. 10 в первой колонке приведены результаты проверки дифференциальных показателей шифра Мухомор со стандартными S-блоками. Результаты тестирования шифров Мухомор со случайными S-блоками приведены в остальных колонках этой таблицы.

Таблица 8

Число циклов	Стандартные подстановки	Усредненное значение для 80 случайных подстановок (10 экспериментов)	Значение для восьми случайных подстановок (1 эксперимент)
1	20	0	0
2	18	25	28
3	18	19,6	20
4	20	18,6	18
5	20	18,8	18
6	20	19,4	20
7	18	18,6	20
8	18	19	18
9	18	19,2	18
10	20	19,6	18
11	20	19,2	20
12	20	19	18
13	18	19,4	20

Таблица 9

Число циклов	Стандартные подстановки	Усредненное значение для 80 случайных подстановок (10 экспериментов)	Значение для восьми случайных подстановок (1 эксперимент)
1	838	815,8	824
2	812	813	810
3	829	820,1	808
4	812	820,6	805
5	907	817,2	840
6	818	827,9	865
7	843	825	790
8	839	835,2	831
9	820	819,4	818
10	818	823	818
11	778	821	904
12	896	818	822
13	825	823,9	842

Таблица 10

Число циклов	Стандартные подстановки	Усредненное значение для 80 случайных подстановок (10 экспериментов)	Значение для четырех случайных подстановок (1 эксперимент)
1	18	19,8	20
2	18	19,4	20
3	18	19,2	20
4	20	18,6	18
5	20	19,8	18
6	18	19,6	20
7	18	18,8	20
8	18	19,6	20
9	20	19	20
10	20	18,8	18
11	20	19,8	22
12	20	19,2	22
13	18	18	20

В табл. 11 представлены линейные показатели этого шифра.

Таблица 11

Число циклов	Стандартные подстановки	Усредненное значение для 80 случайных подстановок (10 экспериментов)	Значение для четырех случайных подстановок (1 эксперимент)
1	833	819,3	813
2	843	830,3	861778
3	818	823,9	855800
4	817	815,8	831
5	835	821,3	804
6	895	810,3	819
7	833	826	835
8	799	812,4	834
9	837	823,8	795
10	817	830	796
11	847	825	802
12	830	839	813
13	833	803,5	816

Выводом из приведенных результатов является возможность использовать случайные S- блоки для реализации эффективного шифрующего преобразования.

S-блоки для шифра Лабиринт

В последней серии экспериментов представляем еще один из шифров прошедшего украинского конкурса – шифр Лабиринт.

И для него приводятся дифференциальные и линейные показатели при использовании в шифре родных и случайно взятых S-блоков.

Таблица 12

Число циклов	Стандартная подстановка	Усредненное значение для 10 случайных подстановок	Значение для одной случайно выбранной подстановки
1	20	101	104
2	20	19,6	18
3	18	19	18
4	20	18,6	20
5	18	19,6	18
6	20	19	18
7	20	19,4	20
8	20	18,6	20

В табл. 13 представлены линейные показатели шифра Лабиринт, которые свидетельствуют о том, что шифр Лабиринт со случайными S-блоками оказывается вполне конкурентоспособным шифру в авторской разработке.

Таблица 13

Число циклов	Стандартная подстановка	Усредненное значение для 10 случайных подстановок	Значение для одной случайно выбранной подстановки
1	839	832,8	826
2	835	831,4	840
3	826	828,3	881
4	832	817	808
5	880	815,8	851
6	829	774,2	798
7	827	830	851
8	786	828	843

Как и для предыдущих шифров, видим, что законы распределения обеих таблиц для случайно выбранных подстановок близки к аналогичным законам распределения для стандартных подстановок.

Выводы

Результатами работы подтверждено центральное положение новой методологии оценки стойкости блочных симметричных шифров к атакам линейного и дифференциального криптоанализа, состоящее в том, что показатели стойкости БСШ не зависят от используемых в шифрах S-блоков, а определяются показателями случайных подстановок соответствующей степени. Более того, показано, что в качестве S-блоков, позволяющих реализовать эффективное шифрующее преобразование, могут выступать S-блоки, выбранные случайным образом. Это значит, что задача поиска математических конструкций совершенных S-блоков, которой уделяется большое внимание в современной криптографической литературе, потеряла практический смысл.

Предложены конструкции случайных S-блоков для шифра Rijndael и шифров, представленных на украинский конкурс, которые по криптографическим показателям не уступают S-блокам, представленным в спецификациях шифров.

Получил дальнейшее развитие метод оценки эффективности оценки криптографических преобразований (итеративных шифров), основанный на оценке числа циклов, необходимых шифру для перехода к дифференциальным и линейным показателям, свойственным случайной подстановке.

Установлено, что по этому показателю криптографической пригодности шифры Калина, Мухомор и Лабиринт, представленные на украинский конкурс, являются более совершенными, чем шифр Rijndael. Они на 1-2 цикла имеют перед ним преимущество в динамике перехода к стационарным состояниям, свойственным случайным подстановкам соответствующей степени.

Список литературы: 1. *Lisitskaya, I.V.* Importance of S-Blocks in Modern Block Ciphers / I.V. Lisitskaya, A.A. Nastenko and K.E. Lysytskiy // Computer Network and Information Security. – 2012. – № 10, 1-12. 2. *Лисицкая, И.В.* Большие шифры – случайные подстановки / И.В. Лисицкая, А.А. Настенко // Радиотехника. – 2011. – Вып. 166. – С. 50-55. 3. *Лисицкая, И.В.* Дифференциальные свойства шифра FOX. / И.В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 122-126. 4. *Горбенко, І.Д.* Перспективний блоковий симетричний шифр “Калина” – основні положення та специфікації / І.Д. Горбенко, В.І. Долгов та ін. // Прикладна радіоелектроніка. – 2007. – Т.6. – № 2. – С. 195-208. 5. *Горбенко, І.Д.* Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов та ін. // Прикладная радиоэлектроника. – 2007. – Т. 6, №2. – С. 147-157. 6. *Головашич, С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. – 2007. – Т. 6, №2. – С. 230-240. 7. *Олейников, Р.В.* Результаты анализа алгоритма шифрования ADE / Р.В. Олейников, В.И. Руженцев, М.С. Михайленко, А.Б. Небывайлов // Прикладная радиоэлектроника. – 2008. – Т. 7, № 3. – С. 210-214.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 25.09.2012