СОДЕРЖАНИЕ

ЛИНЕЙНЫЙ И ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ S-БЛОКОВ

Н. А. Капалова, Д. С. Дюсенбаев, К. Т. Алгазы

Институт информационных и вычислительных технологий МОН РК

Получены S-блоки для алгоритма блочного шифрования для всех неприводимых многочленов восьмой степени. Разработана программа, реализующая проведение линейного и дифференциального криптоанализа для такого типа S-блока. С помощью этой программы проводились исследования S-блоков DES, ГОСТ 28147-89, ГОСТ Р 34.13-2015, AES (Rijndael) и проводилось сравнение результатов.

Ключевые слова: S-блок, линейный криптоанализ, дифференциальный криптоанализ.

На данный момент изучение свойств S–блоков и способов их усовершенствования является одной из главнейших задач в области разработки симметричных блочных алгоритмов шифрования.

Размер *S*-блока является одной из важных характеристик. S-блок размером $n \times m$ предполагает -битовые входные значения и m-битовые выходные. Устойчивость алгоритма определяется размером S-блока, чем он больше, тем выше стойкость по отношению к методам линейного и дифференциального криптоанализа, а также ее равномерностью. В зависимости от размера S-блока, усложняется его проектирование. Исходя из практических соображений, значение n, как правило, выбирают в диапазоне от 8 до 10 [1,2].

Найберг К. предложил использовать следующие подходы при разработке S-блоков:

– Случайный выбор. Элементы S–блоков выбираются с помощью генератора или специальных таблиц псевдослучайных чисел. В случае небольшого размера (6x4) такой способ может привести к созданию S-блоков с нежелательными характеристиками, но для больших блоков (8x32) он должен быть вполне приемлемым.

– Случайный выбор с проверкой. Элементы S-блока выбираются случайным образом, но после этого полученные результаты должны проверяться на соответствие различным критериям, описанным выше, с отсеиванием тех матриц, которые не выдержали такой проверки.

– Выбор вручную. Элементы S-блока выбираются практически вручную с использованием элементарных математических преобразований. Для больших S-блоков использование данного подхода сопряжено с немалыми трудностями.

– Математический подход. Элементы S-блока генерируются на основе тех или иных математических принципов. Такой подход обеспечивает S-блоки, гарантирующие заданный уровень надежности по отношению к методам линейного и дифференциального криптоанализа, а также хорошие показатели диффузии (то есть рассеивания статистических особенностей открытого текста по широкому диапазону статистических характеристик шифрованного текста).

Разработана программа, реализующая проведение линейного и дифференциального криптоанализа для любых S-блоков симметричного алгоритма. С помощью этой программы проводились исследования S-блоков DES, ГОСТ 28147-89, ГОСТ Р 34.13-2015, AES (Rijndael). Проведен также линейный и дифференциальный криптоанализ операции умножения многочленов в НПСС [3].

В ходе линейного криптоанализа S-блока прослеживаются всевозможные комбинации двоичных векторов входа и выхода. Каждую пару векторов используют в качестве маски,

которую накладывают на всевозможные пары вход-выход блока замены. Эти маски указывают нам биты входа и выхода соответственно, которые необходимо поразрядно сложить по модулю два, а затем вычислять количество единиц. Полученные данные заполняем в таблицу и определяем элементы, имеющее наибольшее отклонение от половины числа всех возможных комбинаций входных векторов в двоичной системе.

Дифференциальный криптоанализ S-блока рассматривает количество зависимостей разностей входов, соответствующих разностям выходов. Таблицы результатов анализа S-блоков DES совпадает с известными результатами [1].

Одной из функций программы является разработка S-блоков с хорошими характеристиками. Были проверены полученные *S*-блоки для всех неприводимых многочленов восьмой степени. Эти *S*-блоки основаны на получении обратных элементов относительно умножения в поле GF(2^8). К полученным обратным многочленам прибавляются выбранные определенным образом многочлены. Проверено, что такие S-блоки одинаково стойки и к дифференциальному и к линейному криптоанализу.

Например, с помощью неприводимодимого многочлена $x^8 + x^6 + x^3 + x^2 + 1$ и воспомогательный многочлен $x^7 + x^6 + x^3 + x$ для построения блока замены (*S*-блок), который приведен в табл. 1. В нем старшие четыре бита показывают строки таблицы, а младшие четыре бита показывает столбцы. Для удобства этот *S*-блок обазначим *S7.101*.

Таблица 1 – S-блок S7.101

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	202	203	108	14	153	77	168	190	69	230	47	238	251	148	240	183
1	43	225	220	58	30	71	216	59	116	249	229	21	215	214	82	38
2	28	85	121	73	193	46	178	5	160	139	42	219	195	68	20	208
3	149	198	117	211	123	154	3	17	98	94	196	182	134	36	188	177
4	161	227	35	110	53	163	45	144	105	147	184	125	246	37	11	41
5	255	122	76	206	186	6	100	102	104	131	141	44	165	0	199	250
6	67	18	204	191	51	112	96	56	52	143	226	138	8	23	1	150
7	158	7	128	124	205	169	244	176	236	4	189	245	241	197	81	26
8	89	65	120	233	24	126	152	207	19	170	88	75	31	223	231	194
9	61	114	64	74	243	99	55	32	212	39	27	180	12	62	29	235
10	118	48	146	130	137	34	200	15	242	95	172	57	157	101	156	103
11	155	254	72	232	79	25	185	129	91	60	175	50	106	49	210	248
12	40	132	166	22	201	109	86	63	16	252	151	164	159	187	179	237
13	181	80	78	127	222	70	234	84	171	66	2	253	9	167	228	209
14	224	218	10	133	239	192	145	140	111	136	93	54	213	83	247	135
15	217	221	173	97	87	13	115	90	113	174	107	119	33	92	162	142

Результаты линейного и дифференциального криптоанализа сравнивались между собой на равномерность. В табл. 2 показаны результаты линейного и дифференциального криптоанализа по операции умножения многочленов в НПСС для неприводимых многочленов восьмой степени [4].

Таблица 2 – Интервал результатов линейного и дифференциалного криптоанализа

Наименование		Минимум	Максимум	средний минимум	средний максимум	Хи-квадрат	степень свободы
DES	Линейный	12	48	15,5	46,25	480	944
	Дифференциалный	0	16	0	16	20514	1007
ГОСТ 28147-89	Линейный	2	14	2,75	13,75	120	224
	Дифференциалный	0	8	0	6,25	480	239
ГОСТ Р 34.13-2015	Линейный	100	156			32640	65024
	Дифференциалный	0	8			111297	65279
AES-128 (Rijndael)	Линейный	111	145			32639	65024
	Дифференциалный	0	5			67125	65279
НПСС	Линейный	128	256			32640	65024
	Дифференциалный	0	256			16646400	65279
S7.101	Линейный	112	144			32640	65024
	Дифференциалный	0	4			67320	65279

По результатам исследования (табл. 2) можно сделать следующие выводы. Для того чтобы *S*–блок был стойким к линейному криптоанализу, элементы матрицы, полученные в результате линейного анализа, должны принимать значения, близкие к половине количества всех возможных комбинаций входных векторов в двоичной системе. Для того чтобы *S*–блок был стойким к дифференциальному криптоанализу, элементы разностной матрицы, полученные в ходе дифференциального анализа, должны принимать значения, близкие к единице.

Исследованные *S*–блоки показали хорошие статистические свойства, из этого вытекает, что разработанные *S*–блоки ни и чем не уступают *S*-блокам известных стандартов.

Разработан программный продукт «S-блок», который предназначен для проведения дифференциального и линейного криптоанализа S-блоков, а также для создания S-блоков по неприводимым многочленам с обратными элементами (рис. 1).

Алгоритм реализации работы программы для создания S-блоков:

1. Вводятся неприводимый многочлен в поле со списком «Неприводимый многочлен», многочлен в текстовые поля «Вектор» и матрица в текстовые поля «Матрица»;

2. По нажатию кнопки «Создать S-блок» выполнается создание таблицы замен, т.е. S-блока;

3. Полученные результаты записываются как элементы таблиц «S-блок» в десятичной системе счисления и «S-блок» в шестнадцатеричном виде.

Алгоритм реализации криптоанализа:

1. Ввод анализируемого S-блока в окно программы «S-блок» в десятичной системе счисления;

2. Выбор метода криптоанализа «Линейный» или «Дифференциальный»;

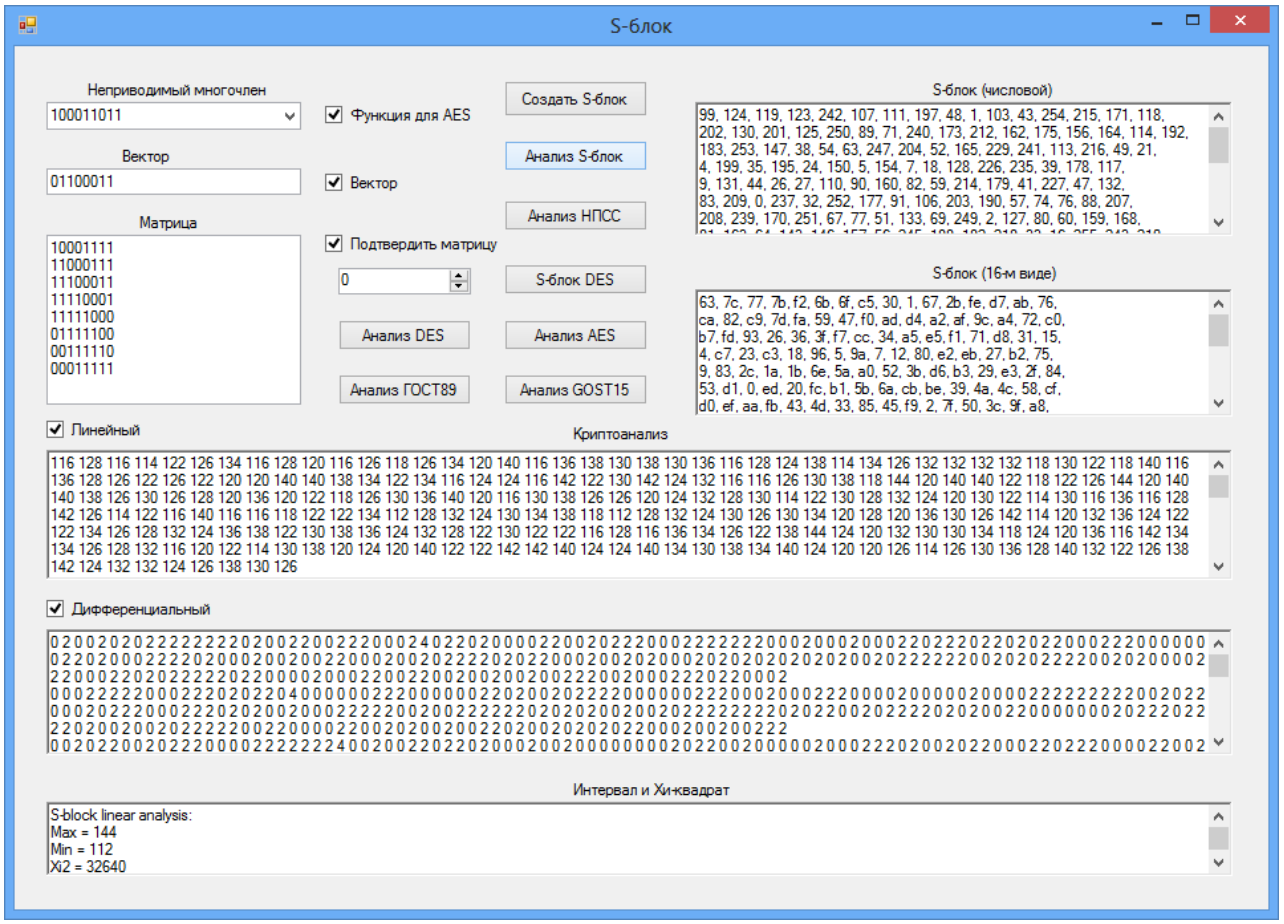

Рис. 1. Главное окно программы «S-блок»

3. Нажатием кнопки «Анализ S-блок» выполнается криптоанализ по выбранному методу анализа в пункте 2;

4. Результаты криптоанализа записываются соответственно в окно «Линейный» или «Дифференциальный»;

5. Выдаются также значения минимальный, максимальный и Хи-квадрат для выбранного метода криптоанализа.

Получены S-блоки для алгоритма блочного шифрования для всех неприводимых многочленов восьмой степени. С помощью разработанной программы проведены линейный и дифференциальный криптоанализ S-блоков. Как показано в таблице 2, результаты криптоанализа *S*–блоков по критерии Хи-квадрат удовлетворительны.

Список литературы

1. Л.К. Бабенко, Е.А. Ищукова. Современные алгоритмы блочного шифрования и методы их анализа // Москва. Гелиос АРВ - 2006.

2. В. Столлингс Криптография и защита сетей: принципы и практика. 2-е изд. / Пер. С англ. - М.:Вильямс, 2001.

3. Амербаев В.М., Бияшев, Р.Г., Нысанбаева С.Е. Применение непозиционных систем счисления при криптографической защите // Изв. Нац. акад. наук Республики Казахстан.- Сер. физ.-мат.– Алматы:Гылым, 2005. - № 3. - С. 84-89

4. Kapalova N., Dyusenbayev D., Security analysis of an encryption scheme based on nonpositional polynomial notations // Journal Open Engineering. - 2016. – 6: C.250-258.

Капалова Нурсулу Алдажаровна – канд. техн. наук, ведущ. науч. сотр. Института информационных и вычислительных технологий МОН РК; 050010, Казахстан, Алматы; e-mail: nkapalova@mail.ru;
Дюсенбаев Дилмуханбет Самуратович – науч. сотр. Института информационных и вычислительных технологий МОН РК; 050010, Казахстан, Алматы e-mail: dimash_dds@mail.ru
Алгазы, Кунболат Тилеуханулы – мл. науч. сотр. Института информационных и вычислительных технологий МОН РК 050010, Казахстан, Алматы; e-mail: kunbolat@mail.ru