УДК 681.3.06

В.И. ДОЛГОВ, Р.В. ОЛЕЙНИКОВ, И.В. ЛИСИЦКАЯ, Р.В. СЕРГИЕНКО, Е.В. ДРОБОТЬКО, Е.Д. МЕЛЬНИЧУК

Харьковский национальный университет радиоэлектроники, Украина

ПОДСТАНОВОЧНЫЕ КОНСТРУКЦИИ СОВРЕМЕННЫХ СИММЕТРИЧНЫХ БЛОЧНЫХ ШИФРОВ

Приведен аналитический обзор критериев построения (отбора) S-блоков современных симметричных блочных шифров на примере алгоритмов КАЛИНА, ADE, МУХОМОР, ЛАБИРИНТ, AES, Fox и Camellia. Отмечено, что S-блоки шифров, для построения которых использована операция возведения в степень над конечным полем, обладают схожими криптографическими показателями, однако являются уязвимыми к алгебраической атаке. В то же время S-блоки БСШ, при конструировании которых отошли от такого рода алгебраических конструкций, обладают несколько ухудшенными показателями стойкости к статистическим методам криптоанализа, но при этом обеспечивают стойкость всего шифра как к статистическим, так и алгебраическим видам криптоанализа. Показано, что большинство рассмотренных S-блоков, как правило, можно отнести к множеству «случайных» подстановок.

Ключевые слова: *S-блок, булевы функции, критерии случайности, линейная аппроксимация, корреляционный иммунитет, δ-равномерность, критерий распространения.*

Введение

Вопросы конструирования S-блоков с высокими криптографическими показателями интересуют специалистов-криптографов уже давно и можно насчитать огромное число публикаций, посвященных этой проблеме. Наиболее плодотворным считается подход, основанный на алгебраических методах описания S-блоков с помощью аппарата булевых функций [1 и др.].

Анализ показывает, что, несмотря на хорошо проработанный математический аппарат, позволяющий выполнить строгое обоснование свойств конструируемых S-блоков, предлагаемые подходы дают решения, ориентированные на определенные классы шифров (например, DES-подобные), часто не лишенные слабостей. В этом отношении более прогрессивным выглядит использование для построения S-блоков отдельных предложений, имеющихся в отмеченных разработках, в частности, предложений К. Ниберг [2 и др.].

Напомним и другой подход отбора подходящих S-блоков [3, 4]. Он строится на основе изучения (определения) показателей случайности блоков подстановок и последующего отбора «хороших» S-блоков из множества случайных с помощью дополнительного статистического тестирования [5].

Нас заинтересовало соотношение названных двух подходов. Ставится задача ответить на вопрос, имеется ли какая-либо связь между ними, и если она существует, то насколько эти подходы могут оказаться полезными друг для друга?

В этой статье основное внимание сосредотачивается на S-блоках шифров, представленных на конкурс по выбору нового стандарта симметричного блочного шифрования Украины, в числе которых шифры КАЛИНА, ADE, МУХОМОР и ЛАБИРИНТ [6-8]. Мы будем также интересоваться и криптографическими показателями S-блоков ряда других известных шифров, таких как AES, Fox и Camellia.

1. Конструкции S-блоков ряда современных шифров

S-блоки шифра Rijndael. Для построения S-блоков шифра AES [9], как уже отмечалось в нашей работе [5], его разработчики Даймен и Раймен за основу взяли отображение $F(x) = x^{-1}$ в конечном поле, скомбинированное с простой аффинной функцией, – конструкцию, предложенную К. Ниберг [2].

S-блоки шифра ADE. В отличие от AES, в шифре ADE [6] используются изменяемые (различные) таблицы блоков замены. По существу, используется такое же преобразование, что и в шифре AES, но в него введен дополнительный параметр $\gamma \in GF(2^8)$, формируемый с помощью битов расширенного мастер-ключа.

S-блоки шифра «Лабиринт». Как отмечает сам автор разработки в [7], S-блок алгоритма выбран из множества так называемых предельно-нелиней-

ных биективных преобразований, в основе которых лежит конструкция Ниберг-Динга, т.е. преобразование, аффинно-эквивалентное функции вычисления обратного элемента в поле $GF(2^8)$.

S-блоки шифров Калина и Мухомор [8]. В шифре «Калина» используется 8 различных подстановок «байт-в-байт», причем для байтов одной строки текущего состояния шифра используется одна и та же подстановка. Разработчики шифра при выборе S-блоков отошли от общепринятых подходов, ориентированных на достижение высоких криптографических свойств булевых функций, составляющих S-блок.

В качестве основного показателя S-блока взято обеспечение его высокой стойкости к алгебраическим атакам, осуществляемым на основе описания криптографических преобразований с помощью систем уравнений (одна из потенциальных слабостей шифра Rijndael использует именно это). Авторы применили в шифре S-блоки, сгенерированные случайным образом. Это исключило возможность задания используемых нелинейных преобразований с помощью системы уравнений, как это легко удается для S-блока шифра Rijndael [9]. Для шифра «Мухомор» указывается, что таблицы подстановок совпадают с первыми 4-мя S-блоками алгоритма «Калина».

S-блоки шифра Camellia. В этом алгоритме подстановочное цикловое преобразование состоит из 8-ми байтовых нелинейных преобразований, составленных из 4-х различных S-блоков. Все они являются аффинными эквивалентами инверсной функции в $GF(2^8)$.

S-блоки шифра FOX. Разработчики S-блоков этого шифра [10] отмечают, что их первичная цель состояла в том, чтобы избежать чисто алгебраической конструкции для S-блока; вторичной целью стала возможность реализации S-блока эффективным путем в аппаратных средствах, использующих ASIC или FPGA технологии. Реализованная ими S-блоковая функция является нелинейным биективным отображением 8-ми битных входных значений в 8-ми битные выходные. Она строится с помощью схемы Лэя-Мэсси с тремя циклами и тремя разными «малыми» (размером 4×4) подстановками.

2. Сравнительная оценка криптографических свойств S-блоков

Методики исследования криптографических свойств S-блоков с помощью аппарата булевых функций и критериев случайности рассмотрены в нашей работе [5], в которой изучались S-блоки уменьшенных моделей шифров. Они были перенесены на S-блоки больших шифров.

Для решения поставленной задачи были разработаны программные комплексы, позволяющие сразу получить две группы криптографических показателей. В одну группу вошли:

- число возрастаний;
- число циклов;
- число инверсий;
- δ-равномерность S-блока;
- максимальное значение линейной аппроксимационной таблицы (LAT);
- наличие фиксированных точек: $S(x) = x$.

В другую группу показателей, основывающихся на алгебраическом описании S-блоков с помощью математического аппарата булевых функций, вошли:

- сбалансированность булевых функций S-блока;
- среднее и минимальное по множеству функций S-блока количество термов АНФ;
- среднее и минимальное по переменным множества функций количество термов:
- корреляционный иммунитет S-блока – $KI(k)$;
- критерий распространения (строгий лавинный критерий) функции – $KP(k)$;
- алгебраическая степень булевых полиномов S-блока – $\deg_f(S)$:

$$\deg_f(S) = \min_{0 \le i < n} \deg(f_i); \quad (1)$$

- абсолютное значение корреляции S-блока – P_S:

$$P_S = \min_f P_f. \quad (2)$$

Для удобства сравнения показатели первой группы расмотренных S-блоков приведены в табл. 1.

В табл. 2 представлены результаты сравнительной оценки свойств рассмотренных S-блоков по второй группе показателей. Что касается сбалансированности, то все S-блоки являются биективными и, следовательно, состоят из сбалансированных булевых функций.

Приведенные в табл. 2 данные свидетельствуют, что булевы функции, входящие в S-блоки, по показателям нелинейности, алгебраической степени и функциям корреляции обладают значениями, близкими к показателям компонентных функций блока нелинейных замен алгоритма AES.

Таблица 1

Оценка S-блоков первой группой показателей

Показатель \ Шифр	AES	ADE	«Лаби-ринт»	«Му-хомор»	FOX	Camellia
Количество циклов	5	9	7	5	8	3
Количество инверсий	16753	15821	16951	15601	17056	15405
кол-во возрастаний	127	125	128	136	125	121
δ-равномерность	4	4	4	8	16	4
Максимум таблицы линейных аппрокс.	16	16	16	30	32	16

Таблица 2

Оценка S-блоков второй группой показателей

Показатель \ Шифр	AES	ADE	«Лаби-ринт»	«Му-хомор»	FOX	Camellia
Нелинейность (min по всем БФ)	112	112	112	98	96	112
Кол-во термов АНФ - в среднем	126,6	128,1	130,5	127,7	117,8	129,6
- минимальное	110	119	124	124	102	126
Количество термов - среднее по функциям и переменным:	62,95	63,87	64,76	62,64	55,77	64,14
- минимальное	50	51	56	54	41	50
Алгебраическая степень (min по всем БФ)	7	7	7	7	6	7
Алгебраическая степень каждой переменной (min по *f*)	7	7	7	7	6	7
КИ (для всех БФ)	0	0	0	0	0	0
КР (для всех БФ)	0	0	0	0	0	0
Векторов, удовл. КИ	16	16	16	26,37	71,25	16
Векторов, удовл. КР	32	32	32	34,25	38,12	32

Алгебраическая степень каждой переменной $\deg(f, x_i)$, как и алгебраическая степень каждой функции $\deg(f)$ являются максимально достижимыми (и гарантируют стойкость к атаке дифференциалов высших порядков). Абсолютные значения корреляций для множества функций каждого из рассматриваемых S-блоков имеют низкие значения (обеспечивают стойкость к корреляционным атакам [11]).

Анализ остальных данных, приведенных в таблице 2, свидетельствует, что распределение числа одночленов для каждой из функций для любой переменной x_i, является фактически равномерным, значения лежат в пределах $\text{term}(f_i)/2 \pm 10$. Как известно, данный показатель обеспечивает стойкость к интерполяционным атакам, и для рассмотренных S-блоков его можно считать достаточно высоким. Количество термов функции, $\text{term}(f_i)$ также является достаточно высоким (110÷145) и обеспечивает стойкость к интерполяционным атакам (количество термов функций лежит в пределах $\text{term}(f_i)/2 \pm 18$.

В то же время, как свидетельствуют приведенные данные, рассмотренные функции не отвечают критерию распространения и не являются корреляционно иммунными (имеют степень 0). Считается [23], что критерий распространения обеспечивает динамические свойства нелинейного преобразования: если замена одного или нескольких бит на входе преобразования приводит с вероятностью 0.5 к изменению выходного состояния, то такая функция имеет хорошие динамические свойства, и наоборот.

Анализ приведенных данных показывает, что булевы функции всех рассмотренных S-блоков имеют низкие динамические и корреляционные свойства, т.е. для большинства входных значений функций существует статистическая зависимость с входными векторами.

Заключение

1. S-блоковые конструкции современных шифров AES и Camellia, уже заработавшие высокую репутацию и поддержку специалистов мирового уровня, а также шифры ADE и Лабиринт, представленные на конкурс по выбору нового стандарта блочного симметричного шифрования Украины, практически обладают идентичными криптографическими показателями и построены на одной и той же алгебраической (регулярной) основе.

2. Для предупреждения возможностей проведения алгебраических атак, рассматриваемых в качестве потенциальных слабостей современного шифра AES, в двух других предложениях, представленных на конкурс по выбору нового стандарта блочного симметричного шифрования Украины (шифры «Калина» и «Мухомор»), предлагается отойти от алгебраических методов конструирования S-блоков. Ценой этого, как следует из представленных результатов, является некоторое ухудшение криптографических показателей, таких как нелинейность и дельта-равномерность, что ведет к снижению запаса стойкости к статистическим атакам дифференциального или линейного криптоанализа на 1 цикл (с 6 циклов до 5 циклов в случае шифра AES). Это не приводит к общему снижению стойкости всего шифра, при этом обеспечивается защита алгоритма от алгебраических атак.

3. Хотя и в литературе уделяется очень большое внимание к развитию и применению для оценки криптографических показателей S-блоков алгебраических методов на основе математического аппарата булевых функций, тем не менее, этот алгебраический подход для рассмотренных конструкций S-блоков не является определяющим. Более того, использованные в современных шифрах S-блоковые конструкции обладают далеко не лучшими, а по ряду показателей и весьма низкими криптографическими свойствами. Реальные конструкции S-блоков строятся, скорее, опираясь на первую группу выделенных в работе криптографических показателей.

4. Представленные результаты свидетельствуют (хотя и не без исключений) о том, что хорошие S-блоки, как правило, можно отнести к множеству «случайных» подстановок и, по-видимому, проверку случайности можно было бы включить в процедуры отбора подстановок с хорошими криптографическими свойствами, однако порождать S-блоки порядка 256 с высокими показателями δ-равномерности, как показывает анализ, является вычислительно очень сложной задачей (для этого требуется практически не реализуемые вычислительные мощности).

Именно поэтому все реальные разработки по построению «больших» S-блоков основываются на методах, которые скорее можно назвать регулярными.

Литература

1. Seberry J. Pitfalls in Designing Boxes (Extended Abstract) / J. Seberry, X.M. Zhang, Y. Zheng // Springer-Verlag, 1998. – P. 383-396.

2. K. Nyberg. Differentially uniform mappings for cryptography. In Advances in cryptology // Proceedings of EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York. – P. 55-65.

3. Горбенко И.Д. Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 / И.Д. Горбенко, И.В. Лисицкая //. Радиотехника: Всеукр. межвед. науч-техн. сб. –Х.: ХНУРЭ, 1997. – Вып. 103. – С. 121-130.

4. Lysytska I.V. The selection criteria of random substitution tables for symmetric enciphering algorithms / I.V. Lysytska, A.S. Koriak, S.A. Golovashich, O.I. Oleshko, R.V. Oleynikov // Abstracts of XXVIth General Assembly. Toronto, Ontario Canada, August 13-21, 1999. – P. 204.

5. Долгов В.И. Сергиенко Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров / В.И. Долгов, А.А. Кузнецов, И.В. Лисицкая, Р.В. Сергиенко // Радиотехника: Всеукр. межвед. науч-техн. сб. – Х. ХНУРЭ, 2008. – Вып. 136. – С. 131-139.

6. Кузнецов А.А. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко // Прикладная радиоэлектроника. – Х.: ХТУРЭ, 2007. – Том. 6, №2. – С. 241-249.

7. Головашич С.А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт» / С.А. Головашич // Прикладная радиоэлектроника. – Х.: ХТУРЭ, 2007. – Том. 6, № 2. – С. 230-240.

8. Горбенко І.Д. Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов и др., // Прикладная радиоэлектроника. – Х.: ХТУРЭ, 2007. – Том. 6, № 2. – С. 147-157.

9. Daemen J. AES proposal: Rijndael / J. Daemen, V. Rijmen 1998 [Електронний ресурс]. – Режим доступу до інформації: http://www.nist.gov/aes.

10. P. Junod. FOX: a new family of block ciphers. In H. Handschuh and A. Hasan, editors, Selected Areas in Cryptography: 11th International

Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004. Revised Selected Papers, volume 3357 of Lecture Notes in Computer Science, Springer-Verlag, 2004. – P. 114-129.

11 Siegenthaler T. Correlation-immunity of nonlinear combining functions for cruptographic applications / T. Siegenthaler // IEEE Transactions on Information Theory. IT-30(5), September 1984. – P. 776-780.

Поступила в редакцию 2.02.2009

Рецензент: д-р техн. наук, проф., зав. кафедрой безопасности информационных технологий И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков, Украина.

ПІДСТАНОВОЧНІ КОНСТРУКЦІЇ СУЧАСНИХ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

В.І. Долгов, Р.В. Олійников, І.В. Лисицька, Р.В. Сергієнко, К.В. Дроботько, Є.Д. Мельничук

Наведено аналітичний огляд критеріїв побудови (відбору) S-блоків сучасних симетричних блокових шифрів на прикладі алгоритмів КАЛИНА, ADE, МУХОМОР, ЛАБІРИНТ, AES, Fox и Camellia. Відмічено, що S-блоки шифрів, для побудови яких використана операція піднесення до ступеня над скінченним полем, мають схожі криптографічні показники, однак вони є вразливими до алгебраїчної атаки. Одночасно S-блоки БСШ, при конструюванні яких відійшли від таких алгебраїчних конструкцій, мають дещо гірші показники стійкості до статистичних методів криптоаналізу, але при цьому забезпечують стійкість всього шифру як до статистичних, так і до алгебраїчних методів криптоаналізу. Показано, що більшість розглянутих S-блоків, як правило, можна віднести до множини «випадкових» підстановок.

Ключові слова: S-блок, булеві функції, критерії випадковості, лінійна апроксимація, кореляційний імунітет, δ-рівномірність, критерій розповсюдження.

SUBSTITUTION CONSTRUCTIONS OF MODERN SYMMETRIC BLOCK CIPHERS

V.I. Dolgov, R.V. Oliynykov, I.V. Lysytska, R.V. Sergienko, E.V. Drobotko, E.D. Melnichuk

Analytical review of S-Box constructing criteria for symmetric block ciphers based on algorithms KALINA, ADE, MUKHOMOR, LABIRINT, AES, Fox и Camellia is given in the article. It is mentioned that S-boxes built using powering operation in the finite filed have closer cryptographic characteristics; however, they are vulnerable to algebraic attack. On the other hand, S-boxes that were designed without those algebraic constructions being used, have worse characteristics relative to statistical cryptanalysis, but they guarantee the strength of the whole cipher to statistical and algebraic methods of cryptanalysis. It is shown that most of considered S-boxes are among the set of «random» substitutions.

Key words: S-box, Boolean functions, criterion of randomness, linear approximation, correlated immunity, δ-uniformity, criterion of dissemination.

Долгов Виктор Иванович – д-р техн. наук, проф., проф. кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники, Харьков, Украина.

Олейников Роман Васильевич – канд. техн. наук, доцент, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники, Харьков, Украина. e-mail: roliynykov@gmail.com

Лисицкая Ирина Викторовна – канд. техн. наук, доцент, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники, Харьков, Украина.

Сергиенко Роман Викторович – аспирант кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники, Харьков, Украина.

Дроботько Екатерина Викторовна – студентка 4 курса факультета компьютерной инженерии и управления Харьковского национального университета радиоэлектроники, Харьков, Украина. e-mail: universalevil@mail.ru

Мельничук Евгений Дмитриевич – студент 3 курса факультета компьютерной инженерии и управления Харьковского национального университета радиоэлектроники, Харьков, Украина.