УДК 621. 391: 519. 2: 519.7

БЛОЧНЫЕ СИММЕТРИЧНЫЕ ШИФРЫ — СЛУЧАЙНЫЕ ПОДСТАНОВКИ. КОМБИНАТОРНЫЕ ПОКАЗАТЕЛИ

В.И. ДОЛГОВ, М.Ю. РОДИНКО

Доказывается, что подстановки, порождаемые блочными шифрами, имеют асимптотически (на полноцикловой длине) законы распределения возрастаний и инверсий, свойственные случайным подстановкам.

Ключевые слова: малая модель шифра, комбинаторные свойства, инверсии, возрастания.

ВВЕДЕНИЕ

Одним из ключевых моментов развиваемой новой идеологии оценки показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа [1] является положение, состоящее в том, что все итеративные шифры асимптотически (при полноцикловой длине) являются случайными подстановками.

В частности это означает, что их комбинаторные показатели (инверсии, возрастания и циклы) подчиняются законам распределения инверсий, возрастаний и циклов, найденным для случайных подстановок.

Естественно, что проверить эти свойства на полномасштабных моделях шифров не представляется возможным. Однако эти свойства можно проверить на уменьшенных моделях, полагая, что с ростом степени подстановки (размером битового входа в шифр) его свойства случайности могут лишь усиливаться.

Здесь мы развиваем подход, предложенный в работе [2], в которой были изучены циклические свойства уменьшенной модели шифра Rijndael, и было установлено, что эта малая модель показывает числовые характеристики (математическое ожидание и дисперсию), характерные для асимптотического нормального закона распределения циклов случайной подстановки. Позднее в работе [3] путем сопоставления законов распределения циклов в подстановках, сгенерированных случайным образом и подстановках, сформированных мини-шифром было показано, что по критерию согласия Колмогорова эти законы практически совпадают. Было отмечено, что следует ожидать и повторения шифрами законов распределения инверсий и возрастаний случайных подстановок. Однако это предположение не было подтверждено вычислительными экспериментами.

Теперь мы хотим в полном объёме обосновать это положение.

1. ЭЛЕМЕНТЫ ТЕОРИИ СЛУЧАЙНЫХ ПОДСТАНОВОК

Свойства подстановок случайного типа изучались многими авторами, например [4, 5]. Здесь мы кратко изложим наиболее принципиальные результаты, на которые будем опираться в дальнейшем. Приведём здесь определения и теоремы, доказанные в работе [4]. Напомним кратко и сопровождающий понятийный аппарат.

Инверсии случайных подстановок

На множестве $n!$ перестановок (подстановок) множества $X = \{1, 2, ..., n\}$ зададим вероятное распределение путем приписывания любой перестановке вероятности $1/n!$.

Будем говорить, что элемент $i_k . \in X$, $1 \le k \le n$ образует r инверсий в перестановке $(i_1, i_2, ..., i_n)$, если он расположен впереди r элементов, имеющих меньшие значения.

Первая теорема, связанная со случайными подстановками, касается числа инверсий η_n случайной равновероятной подстановки:

$$\eta_n = \eta_{1n} + \eta_{2n} + ... + \eta_{nn},$$

где η_{kn} — число инверсий в подстановках n-й степени, образуемых i_k-м элементом.

Теорема 1. Если η_n — число инверсий в случайной равновероятной подстановке степени n, при этом $(\eta_n = \eta_{1n} + \eta_2 + ... + \eta_{nn})$, то случайная величина

$$\eta_n' = \left(\eta_n - n^2/4\right) \Big/ \left(n^{\frac{3}{2}}/6\right) \qquad (1)$$

имеет асимптотически нормальное распределение с параметрами (0,1)

Для нас важными будут еще два результата [3].

Циклы случайных подстановок

Для числа циклов случайной равновероятной подстановки справедлива теорема 2.

Теорема 2. Если ξ_n — число циклов случайно равновероятно выбранной подстановки степени n, то случайная величина

$$\xi_n' = \frac{\xi_n - \ln n}{\sqrt{\ln n}} \qquad (2)$$

имеет в пределе нормальное распределение с параметрами (0,1).

Возрастания случайных подстановок

Элементы a_i и a_{i+1} перестановки $(a_1, a_2, ..., a_n)$ чисел 1, 2, ..., n образуют возрастание, если $a_i < a_{i+1}$, $1 \le i \le n-1$.

Теорема 3. Если θ_n — число возрастаний в случайной перестановке (подстановке) степени n, то при $n \to \infty$ случайная величина

$$\theta_n' = \frac{\theta_n - n/2}{\sqrt{n/12}} \qquad (3)$$

в пределе имеет нормальное распределение с параметрами (0,1).

Этих теоретических сведений уже достаточно, чтобы вернуться к решению поставленной задачи.

Нас в дальнейшем будут интересовать возрастания и инверсии.

2. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ВОЗРАСТАНИЙ МИНИ-ВЕРСИЙ ШИФРОВ

Изложим методику построения закона распределения числа возрастаний для малой версии шифра, в которой длина ключа (блока) равна 16 бит. В этом случае для каждого ключа зашифрования из полного множества всех ключей путем последовательных зашифрований (на одном и том же ключе) создаётся массив всех возможных вариантов зашифрованных блоков данных, начиная с зашифрования нулевого значения блока данных, и так последовательно до последнего значения входного блока данных (равного 2^{16}–1). Тем самым в массиве данных запоминается вторая строка нормализованного представления подстановки (шифрующего преобразования). Число возрастаний в подстановке, как известно, равно сумме числа возрастаний для каждого элемента, представляющего собой количество элементов массива, каждый из которых больше предыдущего элемента. Число возрастаний, полученное для каждой подстановки, записывается в специально созданный для этого файл. Таким образом, мы получаем закон распределения плотности вероятности числа возрастаний для сформированных подстановок. В процессе вычислительных экспериментов для шифра Baby-Rijndael был получен закон распределения возрастаний для 65535 подстановок.

В качестве теоретического закона распределения числа инверсий предлагается рассматривать нормальное распределение с параметрами, определяемыми предельной теоремой 3 ($n/2$– математическое ожидание, $\sqrt{n/12}$ – среднеквадратическое отклонение). Соответственно для $n = 65535$ математическое ожидание равно 32767,5; среднеквадратическое отклонение – 73,9.

Для проверки выдвигаемой гипотезы о соответствии эмпирического распределения теоретическому используем критерий Колмогорова-Смирнова, предусматривающий нахождение максимума разности двух интегральных функций распределения:

$$D_n = \max \left| F_{шифра}(x_k) - F_{теорет}(x_k) \right|.$$

В табл. 1 приведены результаты, полученные для мини-версии шифра Rijndael. В силу значительной вариации диапазона значений возрастаний ([32461;33071]) привести полную таблицу со значениями полученных интегральных законов и их разностей не представляется возможным, поэтому мы приводим лишь значения чисел подстановок для выбранных диапазонов.

Таблица 1

Значения количества возрастаний для шифра Baby-Rijndael

Диапазон возрастаний	Количество подстановок
32461-32512	21
32513-32564	168
32565-32616	1131
32617-32668	4581
32669-32720	11209
32721-32772	17437
32773-32824	16619
32825-32876	9781
32877-32928	3593
32929-32980	852
32981-33032	128
33033-33084	15

На рис. 1 представлены функции распределения плотности вероятности для двух законов (более извилистая кривая соответствует экспериментально полученному закону распределения числа возрастаний для подстановок шифра Baby-Rijndael, гладкая кривая соответствует теоретическому закону (асимптотически нормальному закону распределения для диапазона возрастаний с асимптотически предельными параметрами)).В соответствии с методикой, изложенной в [2], максимальная разность двух интегральных законов получилась равной 0,005045. Для уровня значимости $\alpha = 0{,}05$ из таблицы распределения Колмогорова-Смирнова [3] находим $Q(\lambda_0) = 1 - \alpha = 1 - 0{,}5 = 0{,}95 \to \lambda_0 = 1{,}36$. Тогда для $n = 2^{16}$ выходит $\frac{\lambda_0}{\sqrt{n}} = \frac{1{,}36}{256} = 0{,}00531$. Следовательно, $D_n < \frac{\lambda_0}{\sqrt{n}}$. Гипотеза о том, что значения возрастаний в подстановках, формируемых мини-БСШ, распределены по нормальному закону, подтверждается.

Нами также была предпринята попытка доказать соответствие закона распределения возрастаний в Baby-Rijndael и закона распределения случайных подстановок соответствующей степени, как это было сделано в работе [2] для значений циклов. Однако разность полученных законов составила 0,005747. Это значение хоть и незначительно, но превышает пороговое значение 0,00531, что не позволяет нам принять гипотезу о соответствии закона распределения возрастаний в подстановках Baby-Rijndael закону распределения возрастаний в экспериментально полученных случайных подстановках. Это связано с тем, что

генерация случайных подстановок имеет вероятностный характер, и закон, полученный в одном эксперименте, может удовлетворить гипотезе, а закон, полученный в другом эксперименте – нет. Сравнение, осуществляемое с теоретическим нормальным законом, свойственным случайным подстановкам, является более строгим и не оставляет места сомнениям.

3. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ИНВЕРСИЙ МИНИ-ШИФРОВ

Как и при подсчете возрастаний создаётся массив всех возможных вариантов зашифрованных текстов (строится вторая строка нормализованного представления подстановки). Затем на основе последовательного просмотра и сравнения значений элементов массива с текущим, выбранным для анализа, выполняется подсчет числа инверсий, соответствующего рассматриваемому элементу массива (числа превышений значения текущего рассматриваемого элемента множества значений элементов, стоящих в массиве правее рассматриваемого). Результаты подсчетов числа инверсий для каждого из последовательно выбранных элементов массива нижней строки подстановки суммируется, и, как и в случае с возрастаниями, записывается в файл. Закон распределения инверсий был получен для 65520 подстановок.

Полученные значения инверсий для шифра Baby-Rijndael находятся в диапазоне [1063485006; 1083885006]. В табл. 2 представлены интегральные законы, полученные для ширины интервала дискретности взятия отсчётов числа инверсий, равного 1001000.

Согласно предельной теореме 1 в соответствии с (1) математическое ожидание числа инверсий равно $n(n–1)/4$, среднеквадратическое отклонение – $\sqrt{n^3}/6$. Значения данных параметров при $n = 65520$ равны 1073201220 и 2795178 соответственно.

Из таблицы следует, что максимальная разность двух интегральных законов получилась равной 0,002017. Для уровня значимости $\alpha = 0,05$ из

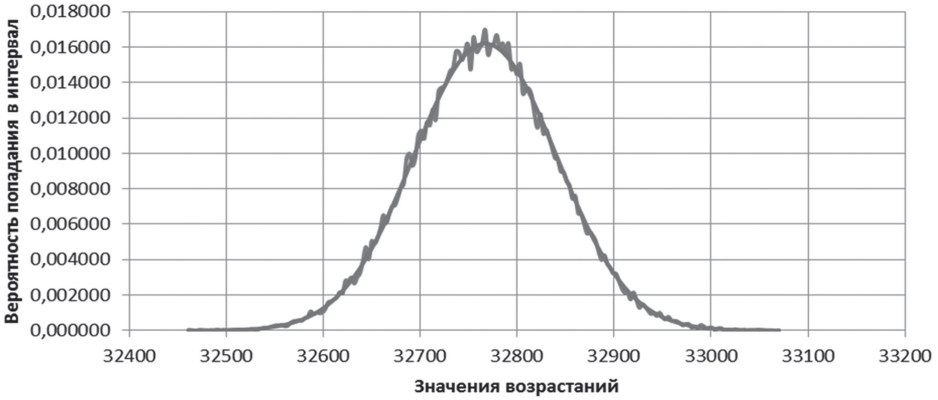

Рис. 1. Экспериментальный и теоретический законы распределения плотности вероятности для числа возрастаний

Таблица 2

Проверка гипотезы о совпадении законов распределения инверсий для шифра и асимптотического нормального закона случайной подстановки

Диапазон инверсий	Количество подстановок	Экспериментальный закон	Теоретический закон	Разность законов
1063606006-1064607006	29	0,000443	0,000569	0,000126
1064607006-1065608006	71	0,001527	0,001889	0,000362
1065608006-1066609006	246	0,005281	0,005568	0,000287
1066609006-1067610006	597	0,014393	0,014606	0,000213
1067610006-1068611006	1289	0,034066	0,034162	0,000096
1068611006-1069612006	2317	0,069430	0,071447	0,002017
1069612006-1070613006	4123	0,132357	0,134073	0,001716
1070613006-1071614006	6061	0,224863	0,226753	0,001890
1071614006-1072615006	7955	0,346276	0,347595	0,001318
1072615006-1073616006	9198	0,486661	0,486413	0,000248
1073616006-1074617006	9167	0,626572	0,626916	0,000343
1074617006-1075618006	8219	0,752015	0,752208	0,000193
1075618006-1076619006	6372	0,849268	0,850647	0,001379
1076619006-1077620006	4464	0,917400	0,918789	0,001389
1077620006-1078621006	2743	0,959265	0,960347	0,001083
1078621006-1079622006	1466	0,981640	0,982678	0,001038
1079622006-1080623006	720	0,992629	0,993249	0,000620
1080623006-1081624006	325	0,997589	0,997658	0,000069
1081624006-1082625006	109	0,999253	0,999278	0,000026
1082625006-1083626006	47	0,999970	0,999803	0,000167
1083626006-1084627006	2	1,000000	0,999952	0,000048

Рис. 2. Закон распределения числа инверсий для шифра мини-Калина

таблицы распределения Колмогорова-Смирнова [6] находим $Q(\lambda_0) = 1 - \alpha = 1 - 0{,}5 = 0{,}95 \rightarrow \lambda_0 = 1{,}36$. Тогда для $n = 2^{16}$ выходит $\frac{\lambda_0}{\sqrt{n}} = \frac{1{,}36}{256} = 0{,}00531$. Следовательно, $D_n < \frac{\lambda_0}{\sqrt{n}}$. Гипотеза о том, что значения инверсий в подстановках, формируемых мини-БСШ, распределены по нормальному закону — подтверждается.

На рис. 2 представлены также результаты построения закона распределения инверсий для шифра Калина, заимствованные из работы [7].

ЗАКЛЮЧЕНИЕ

Таким образом, нами в полной мере обоснован вывод, что блочные шифры на уровне малых моделей по комбинаторным показателям асимптотически являются случайными подстановками. Представляется, что этот вывод полностью переносится и на полномасштабные шифры. Это позволяет в соответствии с методикой, развитой в [1], воспользовавшись формулами, полученными для случайных подстановок, выполнить оценку стойкости полномасштабных БСШ.

Литература

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

[2] Долгов В.И. Анализ циклических свойств блочных шифров. / В.И. Долгов, И.В. Лисицкая, В.И. Руженцев // Прикладная радиоэлектроника. – 2007. – Т.6, №2. – С. 257–263.

[3] Родинко М.Ю., Лисицкий К.Е. Циклические свойства блочных симметричных шифров // Материалы 16-го международного молодежного форума «Радиоэлектроника и молодежь в XXI веке». – 2012. – Т.5. – С. 142–144.

[4] Сачков В.Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982 – 384 с.

[5] Сачков В.Н. Комбинаторные методы дискретной математики. – М.: Наука, 1977. – 319 с.

[6] Бронштейн И.Н., Семендяев К.А. Справочник по математике для инженеров и учащихся Втузов. – М.: Наука, 1980. – 976 с.

[7] Долгов В.И.Криптографические свойства уменьшенной версии шифра – Калина / В.И. Долгов, Р.В. Олейников, А.Ю. Большаков, А.В. Григорьев, Е.В. Дробатько // Прикладная радиоэлектроника, 2010. – Т. 9. – № 3. – С. 349–354.

Поступила в редколлегию 22.03.2013

Долгов Виктор Иванович, доктор технических наук, профессор кафедры «Безопасность информационных технологий» ХНУРЭ. Научные интересы: математические методы защиты информации.

Родинко Мария Юрьевна, студентка кафедры БИТ ХНУРЭ. Научные интересы: технологии блочного симметричного шифрования.

УДК 621. 391: 519. 2: 519.7

Блокові симетричні шифри – випадкові підстановки. Комбінаторні показники / В.І. Долгов, М.Ю. Родінко // Прикладна радіоелектроніка: наук. техн. журнал. — 2013. — Том 12. — № 2. — С. 236–239.

Доводиться, що підстановки, які породжуються блоковими шифрами, мають асимптотично (на повноцикловій довжині) закони розподілу зростань та інверсій, властиві випадковим підстановкам.

Ключові слова: мала модель шифру, комбінаторні показники, інверсії, зростання.

Табл.: 2. Іл.: 2. Бібліогр. 6 найм.

UDC 621.391: 519. 2: 519.7

BBlock symmetric ciphers – random substitutions. Combinatorial indicators / V.I. Dolgov, M.Yu. Rodinko // Applied Radio Electronics: Sci. Journ. —2013. — Vol. 12. — № 2. — P. 236–239.

It is proved that substitutions generated by block ciphers asymptotically have (at monocyclelength) distributions of increases and inversions immanent to random substitutions.

Keywords: small cipher model, combinatorial properties, inversions, increases.

Tab.: 2. Fig.: 2. Ref.: 6 items.