A necessary condition for the feasibility of the schedule was determined. We took into account the behavior of the function graphs to optimize the schedule. We analyzed the mathematical model features including the objective function and the constraints. In the paper we determined the upper and lower limits of total function variation. The possible approaches to solving the optimization problem were introduced. We proposed to solve that task by the branch and bound method. In the proposed approach the objective function is represented as the set or branches included in the method tree.

We developed the algorithm to determine characteristics of the time-step computation process and give a detailed description. The performance of the algorithm was shown by test case.

Key words: discrete optimization, branch and bound, an algorithm.

REFERENCES

1. Korbut A.A., Finkelshteyn Y.Y. Diskretnoe programmirovanie. Moscow, Nauka, Gl.red.fiz.-mat.lit., 1978, 386 p.
2. Hu T. Tselochislennoe programmirovanie i potoki v setyah. Moscow, Mir, 1974, 520 p.
3. Papadimitriu H., Stayglits K. Kombinatornaya optimizatsiya. Algoritmy i slozhnost. Moscow, Mir, 1984, 510 p.
4. Drozdov N.D. Algoritmy diskretnogo programmirovaniya. Uchebnoe posobie TGU. Tver, 2000, 82 p.
5. Ivanov Y.A. Analiz vypolneniya programm pri modelirovanii dinamicheskih sistem, *Naukovi pratsi Donetskogo natsionalnogo tehnichnogo universitetu, Seriya «Problemi modelyuvannya ta avtomatizatsiyi proektuvannya dinamichnih sistem» (MAP-2011)*, No 10 (197), Donetsk, DVNZ «DonNTU», 2011, pp. 234–240.

УДК 621. 391:519.2:519.7

Лисицкая И. В.[1], Настенко А. А.[2]

[1]Канд. техн. наук, доцент Харьковского национального университета радиоэлектроники
[2]Аспирант Харьковского национального университета радиоэлектроники

ДИФФЕРЕНЦИАЛЬНЫЕ СВОЙСТВА БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ С МОДУЛЬНЫМИ ОПЕРАЦИЯМИ ВВЕДЕНИЯ ЦИКЛОВЫХ ПОДКЛЮЧЕЙ, ОТЛИЧАЮЩИХСЯ ОТ XOR

Рассматриваются дифференциальные свойства блочных симметричных шифров с применением разных модульных операций вычисления парных разностей.

Ключевые слова: дифференциальные разности; закон распределения переходов дифференциальной таблицы; поцикловые значения максимумов дифференциалов.

ВВЕДЕНИЕ

Современные блочные симметричные шифры строятся с использованием различных операций введения цикловых подключей. По-видимому, авторы считают, что это помогает усилить криптографическую стойкость алгоритмов шифрования [1, 2]. Хотелось бы найти веские аргументы этому, в частности, представляет интерес в свете большого числа публикаций по оценке максимальных значений дифференциальных вероятностей, выполненных, главным образом, по отношению к шифру Rijndael [3–6 и мн. др.], в котором используется операция введения цикловых подключей с помощью побитного XOR, найти соответствующие оценки для шифров с другими операциями введения цикловых подключей и оценить перспективность их использования.

Будет целесообразным здесь напомнить новый подход к оценке стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, разработанный на кафедре БИТ ХНУРЭ [7], который состоит в оценке соответствующих показателей уменьшенных моделей шифров и определении на основе данных, полученных для уменьшенных моделей, ожидаемых показателей доказуемой стойкости больших прототипов. В ходе реализации этой методики был установлен факт, заключающийся в том, что все итеративные шифры после небольшого начального числа циклов шифрования приобретают дифференциальные свойства случайных подстановок соответствующей степени. Это означает, что интересующие исследователей показатели стойкости могут быть определены расчетным путем из формул, полученных для законов распределения XOR таблиц, выведенных (доказанных) для случайных подстановок [8, 9].

Необходимо отметить, что законы распределения переходов таблиц XOR разностей, построенные для случайных подстановок в известных работах, рассчитывались исходя из предположения, что операцией вычисления разностей пар текстов являлся побитовый XOR «исключающее ИЛИ». Эта операция используется при построении дифференциальных характеристик шифра (дифференциалов) для того, чтобы устранить влияние на построение характеристик цикловых подключей, которые в большинстве блочных симметричных шифров вводятся именно с помощью побитового XOR. Однако, есть немало шифров, где ключ вводится с помощью других модульных операций. Таким образом, встает вопрос об оценке показателей случайности подстановки с отличным от XOR способом вычисления разностей. Это поможет установить ожидаемые значения максимумов дифференциальных вероятностей и для шифров, которые и в этом случае, как ожидается, асимптотически тоже будут повторять свойства случайных подстановок соот-

ветствующей степени, только теперь с иным способом вычисления разностей. В этой работе и ставится задача оценки максимальных значений дифференциальных вероятностей для шифров, использующих отличные от операции XOR способы введения цикловых подключей.

1. МЕТОДИКА ИССЛЕДОВАНИЯ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ ШИФРОВ С РАЗЛИЧНЫМИ МОДУЛЬНЫМИ ОПЕРАЦИЯМИ ВЫЧИСЛЕНИЯ РАЗНОСТЕЙ

Напомним здесь методику исследования дифференциальных свойств шифров, развитую в работе [8]. Она основывается на использовании их полных версий. В частности, в этой работе изучались дифференциальные свойства двух шифров: ГОСТ и Rijndael. Для этих больших версий шифров строились уменьшенные (усеченные) таблицы для 16-битных сегментов открытых и зашифрованных текстов. Было установлено, что оба шифра асимптотически повторяют максимальные значения дифференциальных вероятностей случайных подстановок степени 2^{16}. Результаты этих экспериментов хорошо согласуются и с данными, полученными при исследованиях дифференциальных свойств уменьшенных моделей рассматриваемых шифров [9–12 и др.].

Представляется вполне оправданным использовать данную методику и для построения дифференциальных характеристик шифров с другими операциями введения цикловых подключей, отличающимися от операции XOR, т. е. нас теперь будут интересовать соответственно таблицы дифференциальных разностей, которые будут вычисляться с помощью других модульных операций.

Как и в отмеченном выше подходе, дифференциальные свойства полных версий шифров будем определять, рассматривая 16-битные сегменты входных и выходных разностей, получаемых при зашифровании 2^{16} пар открытых текстов. Такой подход обеспечивает вычислительно реализуемую возможность построения полной таблицы 16-битных разностей. Сами разности будем вычислять для рассматриваемых шифров с помощью операций, обратных операциям введения цикловых подключей.

В качестве объектов исследования будут выступать такие шифры: ГОСТ 28147–89, IDEA и AES. Шифры ГОСТ и IDEA [1, 2] примечательны тем, что в них как раз используются операции введения цикловых подключей, отличные от операции XOR. Для ГОСТ – это операция сложения по модулю 2^{32}. Для IDEA – это операции сложения по модулю 2^{16} и умножения по модулю $2^{16} + 1$, в зависимости от сегмента блока. Для вычисления разностей между парами текстов будут использованы операции, обратные операциям введения подключей. Соответственно, для шифра ГОСТ это будет вычитание по модулю 2^{32}, а для шифра IDEA – вычитание одного сегмента из другого по модулю 2^{16}, а также деление сегментов по модулю $2^{16} + 1$. Однако, прежде чем приступать к изложению результатов исследований, мы остановимся на теоретическом обосновании ожидаемого результата.

2. ЗАКОН РАСПРЕДЕЛЕНИЯ ДИФФЕРЕНЦИАЛОВ СЛУЧАЙНОЙ ПОДСТАНОВКИ С МОДУЛЬНОЙ ОПЕРАЦИЕЙ ВЫЧИСЛЕНИЯ РАЗНОСТЕЙ, ОТЛИЧНОЙ ОТ XOR

В работе [13] приведен вывод соотношения, определяющего закон распределения переходов XOR таблицы случайной подстановки. При его получении было учтено удвоение результатов заполнения ячеек за счет одинакового значения перехода для двух текстов, отличающихся порядком их вхождения в пару блоков данных с одинаковой разностью. Особенностью использования других модульных операций при получении разностей является как раз то, что результаты вычисления разностей будут разными для блоков данных, отличающихся порядком вхождения в разность, т. е. $a - b \neq b - a (\mathrm{mod}\, 2^m)$, также как и $a / b \neq b / a (\mathrm{mod}\, 2^m)$.

Это и нужно учесть при выводе аналитического соотношения для числа переходов дифференциальной таблицы в рассматриваемом случае.

Мы напомним сначала теорему, когда для вычисления разностей применяется операция XOR.

В обозначениях работ [13, 14] пусть $\Pr(\Lambda_\pi(\Delta X, \Delta Y) = 2k$ будет вероятностью того, что значение ячейки дифференциальной таблицы случайно взятой подстановки π степени 2^n для перехода входной разности ΔX в соответствующую выходную разность ΔY будет равно $2k$. Эта вероятность определяется теоремой.

Утверждение 1. *Для любых ненулевых фиксированных* $\Delta X, \Delta Y \in Z_2^n$ *в предположении, что подстановка* π *выбрана равновероятно из множества* S_2^n *и* $0 \le k \le 2^{n-1}$,

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right) = \binom{2^{n-1}}{k}^2 \cdot \frac{k! \cdot \Phi(2^{n-1} - k)}{2^n!}, \quad (1)$$

где функция $\Phi(d)$ определяется выражением

$$\Phi(d) = (2d)! - \sum_{i=1}^{d} (-1)^i \cdot \binom{d}{i}^2 \cdot i! \cdot \Phi(d - i). \quad (2)$$

В работе [14] показано, что хорошей аппроксимацией соотношения (1) является известный из теории вероятностей пуассоновский закон распределения:

$$\Pr(\Lambda_\pi(\Delta X, \Delta Y) = 2k) = \frac{e^{-1/2}}{2^k \cdot k!} \cdot \quad (3)$$

Для этого закона распределения переходов таблицы дифференциальных разностей получено соотношение для определения числа ячеек дифференциальной таблицы, имеющих заполнением число $2k$ в виде:

$$\Lambda_{n,2k} = (2^n - 1)^2 \cdot \frac{e^{-1/2}}{2^k k!} \cdot \quad (4)$$

В этих формулах множитель 2^k, как раз учитывают эффект удвоения разностей при их «симметрии», выполняющейся для операции XOR при разном порядке вхождения блоков данных в пару. Наш анализ показал, что для случая построения дифференциального закона при модульных операциях отличных от XOR, нужные соотношения получаются из выражений (3) и (4) изменением показателя экспоненты на 1 и исключения в этих выражениях множителя 2^k. В результате для интересующих нас соотношений имеем (теперь уже определяются заполнения ячеек без учета удвоения – удвоения нет!):

$$\Pr(\Lambda_\pi(\Delta X, \Delta Y) = k) = \frac{e^{-1}}{k!}, \qquad (5)$$

$$\Lambda_{n,k} = (2^n - 1)^2 \cdot \frac{e^{-1}}{k!}. \qquad (6)$$

Как и в работе [13] максимальное значение переходов случайной подстановки определяется решением уравнения

$$(2^n - 1)^2 \cdot \frac{e^{-1}}{k!} \approx 1.$$

В табл. 1 мы приводим выполненные расчеты по этой формуле вместе с соответствующими результатами расчетов для операции вычисления разностей с помощью побитного сложения по модулю 2 (XOR). Как следует из этой таблицы, в шифрах с модульными (или иными) операциями введения подключей, отличающимися от операции XOR, ожидаемое значение максимума дифференциальной таблицы получается меньше (почти в два раза) по сравнению с шифрами, использующими для введения цикловых подключей операции XOR. Следовательно, использование операций введения цикловых подключей, отличных от операции XOR, действительно приводит к повышению стойкости шифров к атакам дифференциального криптоанализа, однако это улучшение не представляется сколько-нибудь существенным.

Таблица 1. Сравнение расчетных значений для максимумов дифференциальных переходов случайных подстановок различных степеней при разных операциях вычисления разностей

n	Операция mod 2^m, $m > 2$		Операция XOR	
	$\Lambda_\pi(\Delta X, \Delta Y) = 2k$	k	$\Lambda_\pi(\Delta X, \Delta Y) = 2k$	$2k$
4	3,448 0,689	4 5	2,8431 0,3554	6 8
8	4,7462 0,5932	7 8	10,2705 0,8558	10 12
16	3,2984 0,2537	12 13	14,0205 0,7010	18 20
32	2,789 0,1328	20 21	8,159 0,2399	32 34
64	14,4164 0,424	33 34	2,5218 0,0434	56 58
128	1,05009 0,0181	57 58	20,093 0,2051	96 98

Если перейти к показателям доказуемой стойкости, то для 128 битных шифров мы приходим к результатам: $DP^f_{\max} = \frac{98}{2^{128}} = 2^{-121}$ для операции XOR и $DP^f_{\max} = \frac{56}{2^{128}} = 2^{-122}$, например, для операции mod 2^m, $m > 2$.

Теперь можно перейти к экспериментальной проверке этих результатов.

3. АНАЛИЗ ПОКАЗАТЕЛЕЙ СЛУЧАЙНОСТИ ШИФРОВ ПРИ МОДУЛЬНЫХ ОПЕРАЦИЯХ ВЫЧИСЛЕНИЯ РАЗНОСТЕЙ ОТЛИЧНЫХ ОТ XOR

Первые наши эксперименты были выполнены с шифром IDEA. В этом шифре применяются две операции введения подключей: сложение по модулю 2^{16} и умножение по модулю $2^{16} + 1$. Операции в шифре выполняются над 16-битными блоками данных и при построении таблиц разностей мы используем 16-битные сегменты плайнтекстов и шифртекстов над парами которых производятся операции обратные введению подключа, что хорошо подходит к нашей методике.

В табл. 2 приведены средние по 30 таблицам разностей поцикловые значения максимумов этого шифра, для трех операций вычисления разностей, реализованных в шифре: XOR, вычитание по модулю 2^{16} и деление по модулю $2^{16} + 1$ (в IDEA всего 8 циклов зашифрования).

Как видно из представленных результатов, для операций, отличных от XOR, значения максимумов, как и ожидалось, получились меньшими и опять совпадающими с показателями случайной подстановки соответствующей степени. Также как и в случае с XOR-разностями, имеется вполне определенное (стационарное) значение максимума (равное 12), которое устанавливается практически на том же числе циклов, что и значение максимума таблицы XOR-разностей случайной подстановки, и оно сохраняется на всех последующих циклах преобразований. При этом для операции модульного деления стационарное значение максимума приобретается уже на первом цикле (всего на один цикл раньше, чем у двух других операций).

Таблица 2. Поцикловые средние значения максимумов полных 16-битных дифференциалов при различных операциях вычисления разности для БСШ IDEA

Кол-во циклов	Text1 XOR Text2	(Text1 – Text2) mod 2^{16}	(Text1 / Text2) mod $(2^{16} + 1)$
1	1984,134	1383,37	12,1333
2	19,1333	11,9	11,9333
3	19,266	11,9333	12,0333
4	18,9333	11,9667	11,8333
5	19,1333	11,9333	12
6	18,9333	12,0667	12,0333
7	19,066	12	12,0667
8	18,866	11,7333	11,8

В табл. 3 приведены средние по 30 таблицам значения законов распределения переходов для тех же трех операций при полном количестве циклов преобразований шифра IDEA.

Естественно, числа переходов в таблицах разностей для операции модульного сложения (отличной от XOR) и операции деления имеют и нечетные значения (отсутствует механизм удвоения заполнений ячеек, возникающий при операции XOR).

Кроме того, хорошо видно, что распределение переходов в таблицах, построенных с применением операций модульного сложения и деления, отличается от распределения переходов в таблице XOR-разностей. При этом статистика переходов для модульного сложения совпадает со статистикой переходов для модульного деления (немодульные операции, отличающиеся от XOR, ведут себя одинаково).

Далее был поставлен эксперимент с шифром ГОСТ. Этот шифр мы уже рассматривали в работе [8], где приведены поцикловые средние значения максимумов таблиц 16-битных XOR-разностей. В табл. 4 теперь представлены поцикловые средние значения максимумов таблиц разностей, построенных для шифра с применением еще двух, рассматриваемых в данной работе, операций. Операция вычитания по модулю 2^{32}, являющаяся обратной операции введения ключа в шифре ГОСТ, при рассмотрении только младших 16 бит полублока, совпадает с операцией вычитания по модулю 2^{16}. Учитывая, что мы работаем с 16-битными сегментами текстов, столбец для соответствующей операции обозначен как вычитание по модулю 2^{16}. Как видно из результатов, при применении в шифре операции вычитания по модулю 2^{32}, значение максимума 12, которое сохраняется вплоть до последнего цикла, приобретается также как и для операции XOR, с восьмого цикла. Опять-таки, как уже отмечалось в работе [8], значение максимума, равное 12, сохраняется на всех последующих циклах. Напомним, что 8–9 циклов для шифра ГОСТ это показатель глубины лавинного эффекта [16]. Вместе с тем, при использовании операция модульного деления значения максимума приобретается уже на четвертом цикле. В табл. 5 представлены распределения переходов в таблицах разностей, вычисленных на основе 16-битных сегментов открытых текстов и шифртекстов для полного числа циклов шифра ГОСТ. Как видно из этой таблицы, статистика переходов для каждой из трех операций повторяет результаты, полученные для шифра IDEA.

Еще один результат, следующий из выполненных исследований, состоит в том, что как и в случае использования для построения дифференциальной таблицы опе-

Таблица 3. Распределение переходов в таблицах 16-битных дифференциалов шифра IDEA при различных операциях вычисления разности

Значение перехода k	Количество переходов (расчет)	Text1 XOR Text2	(Text1 – Text2) mod 2^{16}	(Text1 / Text2) mod $(2^{16}+1)$
0	$2{,}6049\times10^{9}$	$2{,}60504\times10^{9}$	$1{,}58006\times10^{9}$	$1{,}5801\times10^{9}$
1	–	–	$1{,}58002\times10^{9}$	$1{,}58\times10^{9}$
2	$1{,}30245\times10^{9}$	$1{,}30252\times10^{9}$	$7{,}90014\times10^{8}$	$7{,}89988\times10^{8}$
3	–	–	$2{,}63326\times10^{8}$	$2{,}63329\times10^{8}$
4	$3{,}25612\times10^{8}$	$3{,}25624\times10^{8}$	$6{,}58334\times10^{7}$	$6{,}58329\times10^{7}$
5	–	–	$1{,}31663\times10^{7}$	$1{,}31661\times10^{7}$
6	$5{,}42687\times10^{7}$	$5{,}42666\times10^{7}$	$2{,}19418\times10^{6}$	$2{,}19412\times10^{6}$
7	–	–	313235	313205
8	$6{,}78359\times10^{6}$	$6{,}78211\times10^{6}$	39207	39136,3
9	–	–	4361,8	4302,93
10	678359	678133	436,733	439,067
11	–	–	38,9333	39,4667
12	56529,9	56409,5	3,26667	3,66667
13	–	–	0	0,333333
14	4037,85	4039,2	0	0
15	–	–	0	0
16	252,366	255,067	0	0
17	–	–	0	0
18	14,0203	14,7	0	0
19	–	–	0	0
20	0,701016	0,6	0	0

рации XOR, так и при использовании для построения таблицы других модульных операций закон распределения переходов не зависит от вида операции введения цикловых подключей, применяемых непосредственно в шифре. Значения дифференциальной таблицы зависят (ассимптотически) только от битового размера входа в шифр. Для иллюстрации этого положения в табл. 6 представлены законы распределения 16-битных переходов в таблицах разностей для 256-битного шифра AES, построенные с применением для построения таблиц разностей и операций модульного вычитания и деления, а в самом шифре для введения цикловых подключей применяется операция XOR.

Во второй и третьей колонках этой таблицы представлены результаты расчетов, выполненных по формулам (4) и (6) (во второй колонке для дифференциальной таблицы XOR разностей случайной подстановки, а в четвертой соответствующий закон для разностей, отличных от XOR). Видно, что результаты ничем не отличаются от распределений переходов, полученных при рассмотрении шифров ГОСТ и IDEA. Аналогично выглядят и поцикловые значения максимумов, представленные в табл. 7. Причем, при использовании операции деления по модулю $2^{16}+1$, стационарное значение максимума приобретается на 1 цикл раньше, чем при разностях, формируемых с помощью операций модульного вычитания и XOR.

И без привлечения математических методов оценки близости законов распределения видно, что результаты, полученные экспериментальным путем для всех рассмотренных шифров, практически повторяют соответствующие теоретические законы, т. е. представленные результаты демонстрируют совпадение дифференциальных свойств всех рассмотренных шифров с соответствующими показателями случайных подстановок.

Таблица 4. Поцикловые средние значения максимумов полных 16-битных дифференциалов при различных операциях вычисления разностей для БСШ ГОСТ

Кол-во циклов	Text1 XOR Text2	(Text1 – Text2) mod 2^{16}	(Text1 / Text2) mod $(2^{16}+1)$
1	65536	65536	1079,6
2	65536	65430,1	3800,47
3	64508,5	25376,3	18,8667
4	16674	14012,9	12
5	15038,1	5125,9	11,9
6	212,733	74,8667	12
7	158,533	43,3	12,2
8	19,2667	11,9333	12,0333
9	19,0667	11,8667	11,8667
10	19,1333	11,9	12,0667
11	19,3333	12	12,0667
12	18,7333	12	12,0333

Таблица 5. Распределение переходов в таблицах 16-битных дифференциалов шифра ГОСТ при различных операциях вычисления разности

Значение перехода k	Количество переходов (расчет)	Text1 XOR Text2	(Text1 – Text2) mod 2^{16}	(Text1 / Text2) mod $(2^{16}+1)$
0	$2{,}6049\times10^{9}$	$2{,}60505\times10^{9}$	$1{,}58005\times10^{9}$	$1{,}5801\times10^{9}$
1	–	0	$1{,}58003\times10^{9}$	$1{,}58\times10^{9}$
2	$1{,}30245\times10^{9}$	$1{,}3025\times10^{9}$	$7{,}90012\times10^{8}$	$7{,}89995\times10^{8}$
3	–	0	$2{,}63331\times10^{8}$	$2{,}63325\times10^{8}$
4	$3{,}25612\times10^{8}$	$3{,}25625\times10^{8}$	$6{,}58312\times10^{7}$	$6{,}58329\times10^{7}$
5	–	0	$1{,}31639\times10^{7}$	$1{,}31655\times10^{7}$
6	$5{,}42687\times10^{7}$	$5{,}42695\times10^{7}$	$2{,}19398\times10^{6}$	$2{,}19426\times10^{6}$
7	–	0	313422	313196
8	$6{,}78359\times10^{6}$	$6{,}7828\times10^{6}$	39123	39196,9
9	–	0	4335,53	4363,53
10	678359	678412	444,133	436,133
11	–	0	38,9333	41,3333
12	56529,9	56539,1	3	3,6
13	–	0	0,333333	0,333333
14	4037,85	4025,63	0,0666667	0
15	–	0	0	0
16	252,366	255,367	0	0
17	–	0	0	0
18	14,0203	14,4	0	0
19	–	0	0	0
20	0,701016	0,666667	0	0

Таблица 6. Распределение числа переходов в таблицах 16-битных дифференциалов шифра AES при различных операциях вычисления разности

Значение перехода k	Случайная подстановка (расчет)	Text1 XOR Text2	Случайная подстановка (расчет)	(Text1 – Text2) mod 2^{16}	(Text1 / Text2) mod $(2^{16}+1)$
0	$2{,}6049\times10^9$	$2{,}60505\times10^9$	$1{,}57997\times10^9$	$1{,}58006\times10^9$	$1{,}58011\times10^9$
1	–	0	$1{,}57997\times10^9$	$1{,}58002\times10^9$	$1{,}57999\times10^9$
2	$1{,}30245\times10^9$	$1{,}30251\times10^9$	$7{,}89986\times10^8$	$7{,}9001\times10^8$	$7{,}89996\times10^8$
3	–	0	$2{,}63329\times10^8$	$2{,}63331\times10^8$	$2{,}63328\times10^8$
4	$3{,}25612\times10^8$	$3{,}25622\times10^8$	$6{,}58321\times10^7$	$6{,}58325\times10^7$	$6{,}58311\times10^7$
5	–	0	$1{,}31664\times10^7$	$1{,}31649\times10^7$	$1{,}31667\times10^7$
6	$5{,}42687\times10^7$	$5{,}42683\times10^7$	$2{,}1944\times10^6$	$2{,}19453\times10^6$	$2{,}19383\times10^6$
7	–	0	313486	313067	313459
8	$6{,}78359\times10^6$	$6{,}78321\times10^6$	39185,8	39189,1	39213,1
9	–	0	4353,98	4360,6	4364,8
10	678359	678512	435,398	442,6	435,2
11	–	0	39,5816	40,4	40,4667
12	56529,9	56494,7	3,29847	2,73333	3,73333
13	–	0	0,253728	0,466667	0,4
14	4037,85	4033,33	0	0	0
15	–	0	0	0	0
16	252,366	251,1	0	0	0
17	–	0	0	0	0
18	14,0203	12,8333	0	0	0
19	–	0	0	0	0
20	0,701016	0,933333	0	0	0

Таблица 7. Поцикловые средние значения максимумов полных 16-битных дифференциалов при различных операциях вычисления разности для БСШ AES

Кол-во циклов	Text1 XOR Text2	(Text1 – Text2) mod 2^{16}	(Text1 / Text2) mod $(2^{16}+1)$
1	65536	65536	510
2	3788,8	567,533	11,8333
3	19,266	12,0667	11,9
4	18,866	11,9333	12
5	19,333	12,0333	11,8667
6	19,066	11,9	12
7	18,733	12,1333	11,9667
8	18,933	11,7667	12,0667
9	19,266	11,7	12
10	18,66	11,9667	12
11	19	11,9333	11,9
12	19,066	11,9667	12,0333
13	18,933	11,9667	11,9667
14	19,133	11,9333	11,9333

ВЫВОДЫ

Представленные результаты свидетельствуют, что дифференциальные свойства итеративных блочных симметричных шифров зависят от операции введения цикловых подключей. Опять шифры и при модульных операциях, отличающихся от операции XOR, после небольшого начального числа циклов (а то и сразу) приобретают свойства случайных подстановок соответствующей степени, но теперь уже они приходят к стационарному значению максимума меньшему почти в два раза значения максимума, полученному для операции вычисления разностей в виде побитного сложения блоков данных по модулю 2.

Представленные результаты позволяют сделать вывод о том, что применение операций введения цикловых подключей, отличных от операции XOR, в целом приводит к повышению уровня доказуемой стойкости шифров. Вместе с тем, справедливости ради, можно отметить, что это улучшение не является столь заметным, чтобы его считать определяющим.

Установлено также, что дифференциальные характеристики шифров при вычислении разностей с помощью операций и модульного вычитания, и деления, и побитового XOR не зависят от того, какие действительные операции введения ключевых бит применяются в конкретном шифре.

СПИСОК ЛИТЕРАТУРЫ

1. *Lai, X.* Markov ciphers and differentjal cryptanalysis, Advances in Cryptalogy / X. Lai, J. Massey, S. Murphy //EUROCRYPT'93, LNCS 547, Springer-Verlag. – 1991. – P. 17–38.
2. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ. Государственный стандарт 28147–89. – Государственный комитет СССР по стандартам, 1989.
3. Provable Security against Differential and Linear cryptanalysis for SPN Structure / [S. Hong, S. Lee, J. Lim and other]. – B. Schneier (Ed.): FSE 2000, LNCS 1978, 2001. – P. 273–283.
4. *Baignoires, T.* Proving the Security of AES Substitution-Permutation Network / Thomas Baignoires and Serge Vaudenay // 2004. – 16 p. : http://lasecwww.epfl.ch.
5. AES Security Report. Editors Carlos Cid (RHUL) and Henri Gilbert (FTRD) 30 January 2006, Revision 1.0.
6. *Keliher, L.* Tavares, Completion of computation of improved upper bound on the maximum average linear hull probability for Rijndael / L. Keliher, H. Meijer, and S. Tavares // Technical Report, IACR ePrint Archive (http://eprint.iacr.org, Paper # 2004/074), 2004.
7. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / І. Д. Горбенко, В. И. Долгов, И. В. Лисицкая, Р. В. Олейников // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212–320.
8. *Лисицкая, И. В.* Большие шифры – случайные подстановки. / И. В. Лисицкая, А. А. Настенко // Межведомственный научн. технический сборник «Радиотехника». – 2011. – Вып. 166. – С. 50–55.
9. Криптографические свойства уменьшенной версии шифра «Мухомор» / Лисицкая И. В., Олешко О. И., Руденко С. Н., Дроботько Е. В., Григорьев А. В. // Спеціальні телекомунікаційні системи та захист інформації. Збірник наукових праць. – Київ, 2010. – Вип. 2(18). – С. 33–42.
10. Криптографичекие свойства уменьшенной версии шифра «Калина» / В. И. Долгов, Р. В. Олейников, А. Ю. Большаков [и др.] // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 349–354.
11. Исследование криптографических показателей уменьшенных моделей шифров ГОСТ и DES / В. И. Долгов, Я. А. Макарчук, А. В. Григорьев [и др.] // Прикладная радиоэлектроника. – 2011. – Т.10, № 2. – С. 127–134.
12. Исследование циклических и дифференциальных свойств уменьшенной модели шифра Лабиринт / В. И. Долгов, И. В. Лисицкая, А. В. Григорьев [и др] // Прикладная радиоэлектроника. – 2009. – Т.8, №3 – С. 283–289.
13. Дифференциальные свойства подстановок / Р. В. Олейников, О. И. Олешко, К. Е. Лисицкий [и др.] // Прикладная радиоэлектроника. – 2010. – Т.9, № 3. – С. 326–333.
14. *O'Connor, L. J.* On the Distribution of Characteristics in Bijective Mappings / Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, vol. 795, T. Hellesethed., Springer-Verlag, 1994. – P. 360–370.
15. *Лисицкая, И. В.* Свойства законов распределения XOR таблиц и таблиц линейных аппроксимаций случайных подстановок / И. В. Лисицкая // Вісник Харківського національного університету імені В.Н. Каразіна. – 2011. – Вип. 16, № 960. – С. 196–206.
16. *Шнаер, Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. [Текст] / Б. Шнаер. – М. : ТРИУМФ, 2002. – 816 с.

Стаття надійшла до редакції 24.02.2012.

Лисицька І. В., Настенко А. О.

ДИФЕРЕНЦІАЛЬНІ ВЛАСТИВОСТІ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ З МОДУЛЬНИМИ ОПЕРАЦІЯМИ ВВЕДЕННЯ ЦИКЛОВИХ ПОДКЛЮЧІВ, ЩО ВІДРІЗНЯЮТЬСЯ ВІД XOR

Розглядаються диференціальні властивості блокових симетричних шифрів з застосуванням різних модульних операцій обчислення парних різниць.

Ключові слова: диференціальні різниці; закон розподілу переходів диференціальної таблиці; поциклові значення максимумів диференціалів.

Lysytska I. V., Nastenko A. A.

DIFFERENTIAL PROPERTIES OF SYMMETRIC BLOCK CIPHERS WITH ROUND KEY MODULAR OPERATIONS OTHER THAN XOR

Symmetric block ciphers differential properties with various round key operations are considered. It is shown that known ciphers with round operations other than XOR after small initial encryption rounds acquire random substitution properties of correspondent degree, but they achieve stationary maximal value two times smaller than maximal value acquired for round operation as bitwise XOR. It is concluded that application of round operations other than XOR does not lead to significant growth of provable cipher strength. It is mentioned that all iterative ciphers independently of round key operation type give the same maximal values of full differentials according to difference computation operation as bitwise XOR.

Key words: differences, round key operation, difference transition table distribution law, differential maximum value.

REFERENCES

1. Lai X., Massey J., and Murphy S. Markov ciphers and differential cryptanalysis, Advances in Cryptology – EUROCRYPT'93, LNCS 547, Springer-Verlag, 1991, pp. 17–38.
2. GOST. Gosudarstveny'i standart 28147-89. Sustemy' obrobki informatsii. Zashita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovania. Gosudarstvenny'i komitet SSSR po standartam, 1989.
3. S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon and I. Cho. Provable Security against Differential and Linear cryptanalysis for SPN Structure. B. Schneier (Ed.): FSE 2000, LNCS 1978, 2001, pp. 273–283,
4. Thomas Baignoires and Serge Vaudenay. Proving the Security of AES Substitution-Permutation Network. http://lasecwww.epfl.ch. 2004, p. 16.
5. AES Security Report. Editors Carlos Cid (RHUL) and Henri Gilbert (FTRD) 30 January 2006, Revision 1.0.
6. Keliher L., Meijer H., and Tavares S, Completion of computation of improved upper bound on the maximum average linear hull probability for Rijndael, Technical Report, IACR ePrint Archive (http://eprint.iacr.org, Paper # 2004/074), 2004.
7. Gorbenko I. D., Dolgov V. I., Lisitskaya I. V., Oleinikov R. V. Novaia ideologia otsenki stoikosti blochny'h simmetrichny'h shifrov k atakam differentsialnogo i lineinogo kriptoanaliza, *Prikladnaya radioelektronika*, 2010, Vol. 9, No. 3, pp. 212–320.
8. *Lisitskaya* I. V., Nastenko A. A. Bolshy'e shifry' – sluchainy'e podstanovki, *Mezhvedomstvenny'i nauchn. tehnichesky'i sbornik «Radiotehnika»*, 2011, Issue 166, pp. 50–55.

9. Lisitskaya I. V., Oleshko O. I., Rudenko S. N., Drobat'ko E.V., Grigor'ev A.V. Kriptograficheskyie svoistva umenshenoi versii shifra «Myhomor», *Spetsialni telekomunicatsiini systemy'ta zahist informatsii. Zbirnuk naykovy'h prats'*, Kiiv, 2010, Issue 2(18), pp. 33–42.
10. Dolgov V. I., Oleinikov R. V., Bol'shakov A. Ю., Grigor'ev A.V., Drobat'ko E.V. Kriptograficheskie svoistva umenshenoi versii shifra «Kalina», *Prikladnaya radioelektronika*, 2010, vol. 9, No. 3, pp. 349-354.
11. Dolgov V. I., Makarchuk IA. A., Grigoriev A. V., Drobat'ko E. V. Issledovanie kriptograficheskih pokazateley umensheny'h modeley shifrov GOST i DES, *Prikladnaya radioelektronika*, 2011, Vol. 10, No. 2, pp. 127–134.
12. Dolgov V. I., Lisitskaya I. V., Grigoriev A. V., Shirokov A. V. Issledovanie tsiklicheskih i differentsialny'h svoistv umenshenoi modeli shifra Labirint, *Prikladnaya radioelektronika*, 2009, Vol. 8, No. 3, pp. 283–289.
13. Oleinikov R. V., Oleshko O. I., Lisitskay K. E., Tiviashev K. E. Differentsialny'e svoistva podstanovok, *Prikladnaya radioelektronika*. – 2010, Vol. 9, No. 3, pp. 326–333.
14 O'Connor L. J. On the Distribution of Characteristics in Bijective Mappings. Advances in Cryptology. EUROCRIPT 93, Lecture Notes in Computer Science, vol. 795, T. Hellesethed., Springer-Verlag, 1994, pp. 360–370.
15. *Lisitskaya* I.V. Svoistva zakonov raspredelenia XOR tablits i tablits lineiny'h approksimatsy sluchainy'h podstanovok. [Text], *Visnyk Charkivs'kogo natsionalnogo universitety imeni V. N. Karazina*, 2011, No. 960, Issue. 16, pp. 196–206.
16. *Shnaer* B. Prikladnaya kriptografiya. Protokoly', algoritmy', ishodny'e teksty' na iazuke Si. [Text]. Moscow, TRIUMF, 2002, 816 p.

УДК 004.9

Пшеничний О. Ю.

Аспірант Національного університету «Львівська політехніка»

ВЛАСТИВОСТІ АСОЦІАТИВНИХ ЗАЛЕЖНОСТЕЙ У АНАЛІЗІ ДАНИХ

У статті наведено результати дослідження властивостей асоціативних залежностей та можливостей їх ефективного агрегування. Розрозбено метод виявлення асоціативних залежностей широкого класу у великих наборах даних.

Ключові слова: асоціативна залежність, функціональна залежність, залежності даних, аналіз даних.

ВСТУП

Аналіз даних та отримання з них додаткової інформації про предметну галузь (Data Mining) є на сьогодні великою галуззю комп'ютерних наук, яка активно розвивається і збагачується новими методами, алгоритмами та програмними засобами, що їх реалізовують. Охопити всю структуру та різноманітність підходів даної галузі неможливо.

У даній роботі розглядається задача виявлення асоціативних залежностей у великих обсягах даних та її проблематика, вивчаються можливості оптимізації пошуку асоціативних залежностей та їх властивості.

Аналіз даних на предмет виявлення залежностей та кореляцій широко застосовується у соціології, психології, політології, фізиці, енергетиці, астрономії, комп'ютерних науках та безлічі інших прикладних дисциплін. Задача виявлення асоціативних залежностей в даних соціологічних опитувань розглядається в [1]. Даний напрям аналізу даних відносно не новий, проте в цій галузі до цих пір проводяться активні дослідження. Наприклад, у роботі [2] описується метод побудови агрегованих асоціативних правил на основі простіших залежностей. Пояснити такий інтерес до виявлення залежностей в даних можна стрімким злетом обчислювальної потужності комп'ютерної техніки, а також зростанням обсягів накопичених даних у багатьох галузях життя суспільства до таких обсягів, що аналіз їх експертним шляхом або неможливий, або неповний. Сучасні обчислювальні засоби дозволяють реалізовувати все складніші алгоритми та застосовувати їх до даних великих обсягів. Це стимулює науковців до розробки таких алгоритмів, а власників великих баз та сховищ даних – до розробки програмних засобів аналізу накопиченої інформації.

На даний час деякі науково-технічні галузі вже мають потужні методи аналізу даних, спеціалізовані до своїх потреб та структури даних. Серед них можна виділити програмні засоби CLASSIFI (Department of Pathology, UT Southwestern Medical Center) [3], BiNGO (Department of Plant Systems Biology, VIB/Ghent University) [4] та EASE (National Institute of Allergy and Infectious Diseases) [5]. Проте більшість науково-дослідних установ не можуть дозволити собі розробку подібних систем і потребують загальнодоступного методу широкого застосування.

Отже, ефективний пошук асоціативних залежностей в багатоатрибутних даних є актуальною задачею сучасного аналізу даних.