УДК 621.3.06

АТАКА НА ПОЛНЫЙ ДИФФЕРЕНЦИАЛ УМЕНЬШЕННОЙ ВЕРСИИ БСШ RIJNDAEL

В.И. ДОЛГОВ, И.В. ЛИСИЦКАЯ, Д.Э. ХРЯПИН

Усовершенствуется поход к анализу показателей криптографической стойкости блочных симметричных шифров, строящийся на основе исследования свойств уменьшенных версий этих шифров. Излагаются некоторые результаты применения этой методики для решения задачи определения показателей стойкости шифров к атакам дифференциального криптоанализа. Предлагается решение задачи определения ключа зашифрования уменьшенной модели шифра Rijndael на основе выполнения атаки на полный дифференциал. Результаты обобщаются на оценки показателей стойкости больших шифров.

Ключевые слова: криптографическая стойкость, дифференциальный криптоанализ.

ВВЕДЕНИЕ

В эти дни в Украине проходит конкурс предложений по построению алгоритмов блочного симметричного шифрования, целью которого является отбор претендента на новый стандарт БСШ, взамен используемого до настоящего времени российского шифра ГОСТ 28149-87. Известно, по крайней мере, четыре предложения и сейчас идет их изучение заинтересованными организациями и специалистами.

Опыт показывает, что выполнение экспертизы современного блочного шифра и уровень ответственности при принятии решения является не простой задачей, требующей привлечения значительных временных и интеллектуальных ресурсов. Хотелось бы найти не только убедительные теоретические обоснования, найти которые в криптографии, как правило, очень непросто, но и получить реальные практические результаты, позволяющие собрать данные для сравнительного анализа претендентов. И здесь многие подходы сталкиваются практически во всех случаях с проблемой непреодолимой вычислительной сложности анализа современных БСШ.

Развивается точка зрения, что в значительной степени стоящие трудности можно преодолеть путем разработки и анализа криптографических свойств уменьшенных моделей кандидатов и сопоставления их показателей с показателями уменьшенных моделей известных шифров, которые уже поддаются проведению вычислительных экспериментов. Конечно, при этом необходимо позаботиться, чтобы в уменьшенных моделях были сохранены все основные преобразования и операции прототипов, т.е. чтобы обеспечивалась в известном смысле их ″эквивалентность″ большим прототипам. Некоторые результаты исследований в этом направлении мы уже публиковали в работах [1-4].

Мы хотим здесь напомнить выводы одной из последних наших работ [4], посвященных анализу экспериментов с уменьшенными моделями шифров, позволившему обосновать новую идеологию оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. Было установлено, что:

1. Современные блочные симметричные шифры (при полном наборе шифрующих многоцикловых преобразований) имеют свойства случайных подстановок и для них справедливы законы распределения вероятностей для полных дифференциалов и линейных корпусов свойственные таблицам дифференциальных разностей и линейных аппроксимаций случайных подстановок соответствующей степени. Но если этот результат представляется в некотором смысле ожидаемым, то остальные представляются далеко не очевидными.

2. Максимальные значения полных дифференциалов и линейных корпусов для современных БСШ, определяющие по современным меркам показатели стойкости шифров к атакам дифференциального и линейного криптоанализа, могут быть получены расчетным путем. Они не зависят (при достаточном числе цикловых преобразований ни от свойств используемых в шифрах подстановочных конструкций, ни от методов введения в цикловые функции цикловых подключей, ни от способа построения расширяющего линейного преобразования цикловой функции, а являются функцией только размера битового входа в шифр (порядка подстановки).

3. Для оценки стойкости блочных симметричных шифров с битовым размером входа равным n к атакам дифференциального и линейного криптоанализа справедливы приближенные расчетные соотношения [5, 6]

$$DP^{f}_{\max} = \frac{n+4}{2^{n}}$$

и

$$DL^{f}_{\max} = \left(\frac{\left(\frac{3}{2}\right)^{n}}{2^{n-1}} \right)^{2}.$$

Приведенные формулы позволяют, таким образом, оценить наибольшую вероятность полного дифференциала и линейного корпуса соответственно.

4. На основе анализа результатов проверки показателей стойкости уменьшенных моделей

шифров, представленных на украинский конкурс по выбору кандидата на национальный стандарт БСШ (7-10), сделан вывод, что все шифры, представленные на конкурс, имеют практически и теоретически одинаковые показатели стойкости к атакам дифференциального и линейного криптоанализа.

В соответствии с существующей точкой зрения максимальные значения дифференциальных и линейных вероятностей (максимальных вероятностей полных дифференциалов и линейных корпусов) непосредственно связаны со сложностью соответствующих криптоаналитических атак на шифры. Хотелось бы более глубоко осознать эту связь. Здесь возникает, по крайней мере, три вопроса, на которые хотелось бы получить ответы. Первый вопрос: если мы знаем характеристику (линейную или дифференциальную), соответствующую максимально вероятной, то можно ли на нее построить атаку и как? Конечно, же, найти максимально вероятную характеристику для большого шифра сама по себе сложная (возможно и невыполнимая) задача, но тогда можно искать не обязательно максимально вероятную, а заметно отличающуюся от многих других, и тогда спрашивается, какова вероятность найти такую (уменьшенную по сравнению с максимумом) характеристику? И, наконец, есть третий вопрос: имеется ли возможность выполнить атаку на шифр в случае, когда удается найти характеристику (дифференциальную или линейную), замыкающуюся на ограниченное число S-блоков первого или последнего циклов, которая имеет значение, существенно (а может и просто, заметно) превосходящее значения для многих других характеристик?

В этой работе мы попробуем ответить на эти вопросы, опять опираясь на результаты экспериментов с уменьшенными версиями шифров. И здесь мы будем возможность реализации на малые модели шифров атак переборного типа, что делает возможным в деталях познакомиться с особенностями и возможностями реализации таких атак и на большие шифры. В этой работе, в частности, внимание сосредотачивается на особенностях реализации атаки на полные дифференциалы уменьшенных моделей шифров Rijndael и SPN шифра из работы Хеуса. Естественно, что такого типа атаки на большие шифры до сих пор считаются не реализуемыми. Мы проверим истинность и этого предположения.

1. ПОСТРОЕНИЕ АТАКИ НА ПОЛНЫЙ ДИФФЕРЕНЦИАЛ SPN ШИФРА

Реализации малых шифров взяты из Интернета (для шифра Rijndael) и из ранее выполненных нами исследований и разработок [1-4], в основе которых лежат 16-битные модели.

Прежде всего, изложим саму сущность методики построения атаки на полный дифференциал. Вспомним работу Бихама и А. Шамира [5], в которой они описывают стратегию определения битов ключа на входе S-блока последнего цикла на основе анализа информации о прохождения разностей пар текстов через этот S-блок и знания значений самих текстов на входе расширяющей перестановки, предшествующей S-блоку. В рассматриваемом случае у нас нет значений выходов S-блока цикла (при расшифровании на один цикл зашифрованного текста), как это было в примере Э. Бихама и А. Шамира [5]. Поэтому нам остается только сделать ″откат″ на один цикл (расшифрование зашифрованных на неизвестном ключе пар текстов на одном из вариантов возможных ключей) и далее искать продолжение атаки, используя полученные значения разностей (теперь уже на входах S-блоков последнего цикла). И такая ситуация характерна для всех SPN шифров.

Обратим теперь внимание на то, что в итеративных многоцикловых шифрах последние циклы шифрующего преобразования (в сочетании с предыдущими циклами) ведут себя как случайные подстановки, т. е. фактически все входные биты предпоследнего цикла (более точно – последних циклов) являются активными (переходы разностей через последние циклы осуществляются без потери вероятностей в том смысле, что сохраняется закон распределения разностей переходов таблиц цикловых разностей [6]). Это означает, что для любого S-блока выходная разность формируется на основе полного набора возможных пар входов (для ключезависимой функции при сложении множества входов с ключевыми битами происходит перенаименование входов (они принимают новые значения) при сохранении распределения значений разностей между ними. В результате этого просто изменяется распределение выходов по выходным разностям. Поэтому следует считать одинаково (равновероятно) активными все возможные входные разности. Тогда, если мы рассматриваем какое-либо значение выходной разности S-блока последнего цикла (для пары, взятой из множества отобранных пар текстов с заданным значением разности), участвующего в формировании максимально вероятной дифференциальной характеристики, то естественно полагать, что при формировании этой наиболее вероятной характеристики используются переходы S-блока с наибольшими значениями.

Тогда значения выходов для инверсного S-блока (входов этого же S-блока при шифровании) для интересующей нас характеристики можно определить из таблицы XOR разностей задействованного S-блока, просто выбирая из нее значения, являющиеся наибольшими (таких значений может оказаться и не одно).

В результате рассматриваемая задача опять приводится к изложенной в работе [5], т. е. нам известны значения пар текстов с определенной разностью перед их сложением с ключевыми битами, после которого формируются входы в S-блок, а также известно значение разности на выходе S-блока.

И тогда полностью можно воспользоваться рассмотренной в работе [5] стратегией определения ключевых битов.

Перейдем теперь к результатам реализации изложенной стратегии построения атаки на полный дифференциал. Рассмотрим сначала SPN конструкцию в виде модели шифра подстановочно-перестановочной (SPN) структуры из работы [6], представленную на рис.1.

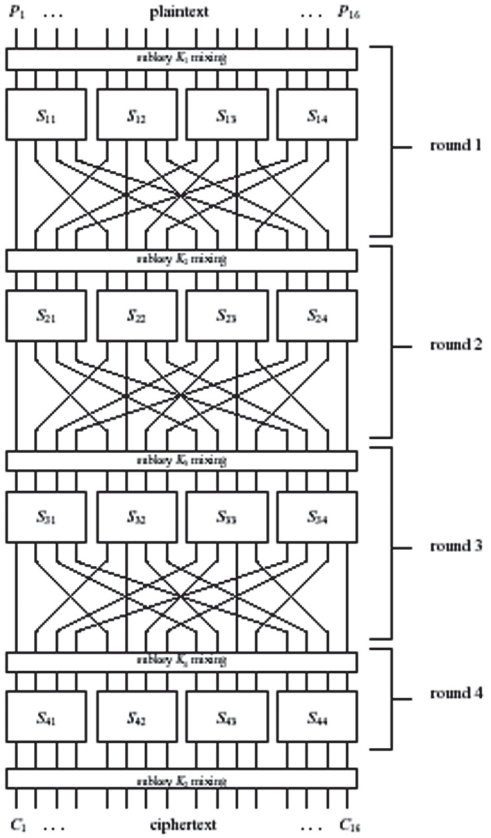

Рис 1. Шифр на основе подстановочно-перестановочной (SPN) структуры

В алгоритме в каждом отдельном цикле преобразований входной 16-битный блок данных делится на четыре подблока, каждый из которых поступает на соответствующие входы блоков замены (S-блоков, осуществляющих замену четырех входных битов на четыре выходных). Естественно, что каждый из блоков замены может быть представлен в виде таблицы, пример которой (мы следуем работе профессора X. Хеуса) представлен в табл. 1 (в данном случае S-блок представляет собой первую строку S-блока алгоритма шифрования DES). На рис.1 наиболее значимый бит шестнадцатеричных значений является самым левым битом выхода каждого S-блока.

Таблица 1

S-блок в шестнадцатеричной системе счисления

Вход	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Выход	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

В нашем эксперименте использовано аналогичное нелинейное преобразование для всех S-блоков.

Таблица 2

Цикловые ключи

1	6	D	1
A	2	7	E
3	9	7	F
F	7	C	6
2	9	0	2

Первым этапом задачи стал поиск максимально вероятной дифференциальной характеристики (полного дифференциала). В нашем эксперименте за основу была взята процедура расшифрования (хотя с одинаковым успехом можно было бы взять и процедуру зашифрования). Для поиска полного дифференциала использовалась та же методика, что и при построении таблиц дифференциальных разностей подстановок [5] (последовательно перебирались пары текстов с фиксированной входной разностью, и подсчитывалось число пар входов с фиксированной входной разностью, которые при расшифровании формировали одну и ту же выходную разность).

После выполнения 4-х цикловой программы с вышеописанными параметрами были получены результаты (для отдельного фиксированного значения мастер-ключа зашифрования при вариации по всему множеству 2^{16} пар текстов для каждой входной разности), представленные в таблице 3.

Таблица 3

Результаты поиска максимально вероятного дифференциала для 4-х циклового шифра

Входная разность (hex)	0505	5415	BB0B
Выходная разность (hex)	B0BB	B0B0	E0A0
Количество повторов (dec)	216	186	44

Для поиска частного (из множества полных) дифференциала (частного в смысле анализа не полного множества дифференциалов, т.е. речь здесь снова шла о полных дифференциалах) использовался фактически тот же алгоритм, только объем вычислений был существенно сокращен (до 2^4 пар текстов). Кроме того, в отличие от первого случая, зашифрование проводилось уже на 8-ми циклах. S-блоки остались прежними (одинаковыми). Цикловые (раундовые) ключи были расширены [см. табл. 4]

Таблица 4

Расширенные цикловые ключи

1	6	D	1
A	2	7	E
3	9	7	F
F	7	C	6
2	9	0	2
B	5	8	4
0	E	A	3
6	B	9	5
8	1	D	7

Результаты, полученные после выполнения программы с указанными параметрами, представлены в таблице 5.

Таблица 5

Результаты выполнения поиска максимально вероятного дифференциала

Входная разность (hex)	7	1	2
Выходная разность (hex)	6583	C890	1FF8
Количество повторов (dec)	12	10	10

Из результатов измерений, представленных в таблицах 3 и 5, следует, что максимально достижимые значения полных дифференциалов для шифра с четырьмя циклами существенно отличаются от соответствующих значений шифра с 8-ю циклами. Это следует и из нашей работы [2 и др.]. Напомним, что как показано в работе [2], SPN шифр рассмотренного типа выходит на ″асимптотические″ значения полного дифференциала (становится случайной подстановкой) лишь при 7-8-ми циклах, в то время как уменьшенная модель шифром Rijndael приходит к потенциальному значению максимума полного дифференциала уже при 4-х циклах.

2. РЕАЛИЗАЦИЯ АТАКИ КРИПТОАНАЛИЗА

Для атаки использовали следующий алгоритм.

Выполняется дешифрование пар шифртекстов, входящих в отобранные пары (реализующие один из выделенных в таблицах переходов) на цикл (раунд) на всех возможных множествах значений ключевых битов, участвующих в формировании выходной (после одноциклового расшифрования) разности (на входе инверсных S-блоков). Затем с помощью счетчиков определяется, для какого из сочетаний ключевых битов получаемые значения разностей совпадают наибольшее число раз с разностями (разностью) на входах (входе) S-блоков (S-блока), следующими (следующей) из таблицы 6.

В данном случае для выходной разности 6583 следует считать наиболее вероятным переходом слоя для S-блоков последнего цикла входную разность 84F1. Результаты выполнения атаки на полный дифференциал (на весь шифр) иллюстрирует таблица 7 естественно, что атака начинается с перехода с максимальной вероятностью.

Таблица 7

Результаты выполнения атаки на полный дифференциал (всего шифра)

Входная разность 4 цикл (hex)	505	5415	BB0B	0066	0B0B
Выходная разность 3 цикл (hex)	202	808	8088	0660	2022
Количество ключей до цикла поиска (dec)	65536	1024	256	16	4
Количество ключей после цикла поиска (dec)	1024	256	16	4	1

Заметим, что при использовании только одной разности не удается достичь однозначного определения подключа последнего цикла (максимальное значение подтверждает множество возможных подключей). Поэтому атака продолжается с использованием множества пар текстов, удовлетворяющих очередной из отобранных пар разностей.

Результаты выполнения атаки на ″частный дифференциал″ иллюстрирует табл. 8

Таблица 8

Результаты и параметры атаки на ″частный дифференциал″

Входная разность 8 цикл (hex)	7	1	2
Выходная разность 7 цикл (hex)	D	D	A
Количество ключей до цикла поиска (dec)	16	4	2
Количество ключей после цикла поиска (dec)	4	2	1

Таблица 6

Дифференциальная характеристика S-блока

		Выходная разность															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Входная разность	**0**	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	2	2	0	2	0	2	0	2	2	0	0	0	0	4	0
	2	0	0	2	2	0	0	0	0	2	4	2	0	2	0	0	2
	3	0	4	0	0	2	0	0	2	2	0	2	0	2	2	0	0
	4	0	2	4	0	0	2	2	2	0	0	2	0	0	0	0	2
	5	0	0	0	0	4	0	2	2	0	2	0	2	2	0	0	2
	6	0	0	0	0	0	2	2	0	4	0	2	2	2	0	2	0
	7	0	0	0	2	0	0	4	2	2	0	0	0	0	2	2	2
	8	0	2	0	2	2	2	0	0	2	0	0	2	0	0	0	4
	9	0	2	0	0	0	2	0	0	0	2	0	0	2	4	2	2
	A	0	2	2	2	0	0	2	0	0	0	0	2	4	2	0	0
	B	0	0	2	2	2	4	0	2	0	0	0	0	2	0	2	0
	C	0	0	0	2	2	2	2	0	0	2	4	0	0	2	0	0
	D	0	0	2	0	2	0	0	0	0	0	2	4	0	2	2	2
	E	0	2	0	4	0	0	0	2	0	2	2	2	0	0	2	0
	F	0	0	2	0	0	2	0	4	2	2	0	2	0	2	0	0

На рис. 2 представлена сравнительная диаграмма, иллюстрирующая процесс устранения неопределенности с использованием 3-х возможных разностей.

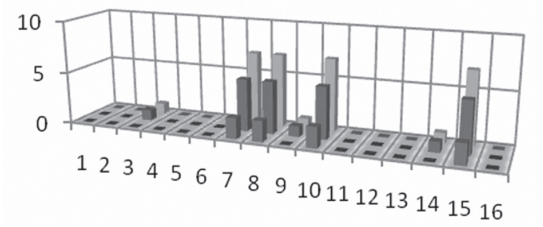

Рис. 2. Сравнительная диаграмма устранения неопределенности с использованием трех возможных разностей

В результате видно, что искомая разность третья, а вероятные ключевые биты (полубайты) 7,8,10,15 (7,8,A,F_h).

Криптоанализ уменьшенной 8-цикловой модели шифра Rijndael.

Мы здесь воспользовались уже имеющейся в Интернете разработкой уменьшенной модели шифра Rijndael [8], только число циклов было увеличено до 9-ти (8-мь и последний цикл неполный).

Для проведения дифференциального криптоанализа и в этом случае сначала изучались частные дифференциальные характеристики, начиная с минимального размера входного блока данных (полубайта), с дальнейшим увеличением размера входного блока до байта.

В качестве ключа использовали следующую таблицу, полученную при помощи алгоритма разворачивания ключей, описанного в [3].

Таблица 9

Последовательность цикловых подключей алгоритма зашифрования baby Rijndael

№ цикла	Ключ			
0	1	2	3	4
1	1	0	2	1
2	4	5	5	7
3	2	6	3	6
4	8	A	C	F
5	7	F	5	9
6	A	D	2	7
7	3	9	4	6
8	1	2	B	F
9	A	B	9	2

При анализе каждого из возможных 4-х битных блоков результат был одинаковый: максимальное значение – это 2 (симметричные) пары текстов, которые дают одинаковое значение выходной разности. При активации 2-ух (правых) S-блоков для 24 дифференциалов на выходе алгоритма шифрования нашлось 4 пары текстов, которые дали одинаковые значения выходной разности (на входе алгоритма шифрования). Ниже перечислены значения дифференциалов на выходе шифра при активации 2 левых S-блоков:

02, 08,13, 1B, 47, 55, 66, 68, 6A, 6B, 88, 9F, A4, A6, A9, AB, B8, B, CD, CF, D0, D4, F4, FC.

При активации 2 левых S-блоков появился один точный максимум для пары разностей Δx = 082C, Δy = 0300. Количество пар текстов удовлетворяющих этой разности равно 6. Эти тексты приведены в таблице 10.

На втором этапе, методом перебора всех ключей, в рабочем диапазоне (2^8), выбираются те, которые дают промежуточную дифференциальную характеристику (на входе последнего S-блока) совпадающую с характеристикой, полученной при анализе таблицы переходов S-блоков.

Таблица 10

Пары текстов с выходной разностью 6

№ пары	Пара текстов	
1	1400	1700
2	1700	1400
3	4C00	4F00
4	4F00	4C00
5	A500	A600
6	A600	A500

Исследуемое выходное значение разности равно 3. По таблице определяем, что вероятней всего на входе S-блока значение разности будет 6 или E. Проведем поиск ключей устраивающих обе пары разностей. Оба поиска отобразим на рисунке ниже.

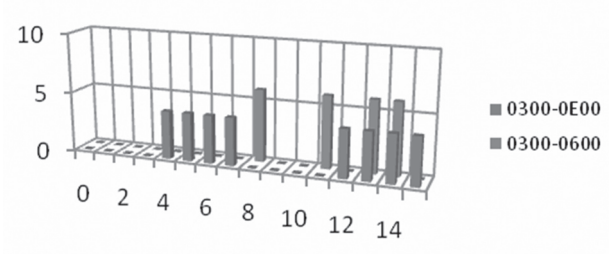

Рис. 3. Сравнительная диаграмма устранения неопределенности с использованием двух возможных разностей

Из рисунка видно, что правильным значением промежуточной разности является 6. Из рисунка также видно, что из 16 возможных ключей (фактически мы все-таки задействовали всего 1 S-блок) осталось только 4. Для продолжения криптоанализа, повторили 2 этап, но для другой разности (число текстов для новой пары разностей уже может быть меньше, но от него зависит качество отсеиваемых ключей). В дальнейшем для уточнения ключа использовались следующие пары:

$$\Delta x = \text{CD57} \rightarrow \Delta y = 0100;\ n = 4\ \Delta z = 0500,$$
$$\Delta x = \text{ABAA} \rightarrow \Delta y = 0\text{F}00;\ n = 4\ \Delta z = 0300.$$

Двукратное повторение 2 этапа позволяет уменьшить количество возможных ключей до 2-х (xBxx, xCxx). В результате общее количество возможных ключей сократилось с 256-ти до 32-х (т.е. в 8 раз). Дальнейшее сокращение количества возможных ключей было выполнено за счет оп-

ределения других байтов ключа Для определения старшего байта ключа, необходимо выбрать такую пару разностей, у которой 2-й байт на выходе алгоритма шифрования будет отличен от 0.

ЗАКЛЮЧЕНИЕ

Общим итогом работы является обоснование и демонстрация принципов реализации атаки на полный дифференциал SPN шифра.

Самый главный результат состоит в том, что атака дифференциального криптоанализа на блочный итеративный шифр может быть построена и на значение полного дифференциала существенно меньшее, чем максимальное значение полного дифференциала, на которое ориентируются при оценке стойкости блочных шифров.

В результате мы приходим к выводу, что все ж совсем не маловажное значение в возможности осуществления атаки дифференциального криптоанализа на SPN шифр играют дифференциальные свойства S-блоков. Они должны быть выбраны так, чтобы таблица XOR разностей не имела существенных отличий от среднего значения случайной подстановки.

От этого, правда, не меняется результирующий закон распределения разностей (полных дифференциалов) преобразования. И поэтому все равно будут существовать выбросы (значения переходов), которые можно пытаться использовать для атак.

Литература.

[1] *Долгов В.И., Лисицкая И.В., Григорьев А.В., Широков А.В.* Исследование циклических и дифференциальных свойств уменьшенной модели шифра "Лабиринт". // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2009. Т. 8, № 3, С. 283-289.

[2] *Долгов В. И., Лисицкая И. В., Киянчук Р. И.* Rijndael – это новое или хорошо забытое старое? Сборник трудов Первой Международной научно-технической конференции "Компьютерные науки и технологии", 8-10 октября 2009г., Белгород, Ч. II, С. 32-35.

[3] *Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Олешко О.И.* Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES // Прикладная радиоэлектроника. – 2009. – Т.8 – №.3, С. 252-257.

[4] *Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев А.Д.* Дифференциальные свойства случайных подстановок. // Прикладная радиоэлектроника. – 2010. Т. 9, № 3. – С. 326-333.

[5] Eli Biham, Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystem, Journal of Cryptology, Vol. 4, 1991. pp.3-72.

[6] *Горбенко И.Д., Долгов В.И., Лисицкая И.В, Олейников Р.В.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. // Прикладная радиоэлектроника. – 2010. Т. 9, № 3. – С. 312-320.

[7] *Horst Feistel.* Cryptography and Computer Privacy // Scientific American. – May 1973. – Vol. 228, No.5. – pp. 15-23.

[8] A Description of Baby Rijndael. ISU CprE/Math 533; NTU ST765-U February 19, 2003.

Поступила в редколлегию 9.07.2010.

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

Лисицкая Ирина Викторовна, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

Хряпин Дмитрий Эдуардович, студент кафедры БИТ ХНУРЭ. Область научных интересов: криптоаналитические свойства БСШ, симметричные криптосистемы и протоколы.

УДК 621.3.06

Атака на повний диференціал зменшеної версії БСШ Rijndael / В.І. Долгов, І.В. Лисицька, Д.Е. Хряпін // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 355–360.

Удосконалюється підхід до аналізу показників криптографічної стійкості блочних симетричних шифрів, побудованих на базі дослідження якостей зменшених версій цих шифрів. Викладаються деякі результати застосування цієї методики для рішення задачі визначення показників стійкості шифрів до атак диференційного криптоаналізу. Пропонується рішення задачі визначення ключа шифрування зменшеної моделі шифру Rijndael на базі виконання атаки на повний диференціал. Результати узагальнюються на оцінки показників стійкості великих шифрів.

Ключові слова: криптографічна стійкість, диференціальний криптоаналіз.

Табл. 10. Іл.03. Бібліогр.: 08 найм.

UDK 621.3.06

Attack on the full differential of reduced version of block symmetric cipher Rijndael / V.I. Dolgov, I.V. Lisitskaya, D.A. Hryapin // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 355-360.

An approach to analyzing the properties of the cryptographic stability of block symmetrical ciphers, which is formed on the base of researching characteristics of the reduced version of these ciphers is improved. Some results of using these methods for solving the problem of determining the indices of the strength of ciphers to differential cryptanalysis attacks are given. A solution to the problem of determining the encryption key of the reduced cipher Rijndael model on the basis of performing a full differential attack is suggested. Results are generalized on estimations of the strength indices of big ciphers.

Key words: cryptographic strength, differential cryptanalysis.

Tab. 10. Fig. 03. Ref.: 08 items.