УДК 621. 3.06

В.И. ДОЛГОВ, д-р техн. наук; А.А. НАСТЕНКО

О РОЛИ СХЕМ РАЗВОРАЧИВАНИЯ КЛЮЧЕЙ В АТАКАХ НА ИТЕРАТИВНЫЕ ШИФРЫ

Ведение

Вопрос о роли схем разворачивания ключей в атаках на итеративные шифры давно считается одним их актуальных в криптографии. Название статьи повторяет название работы [1], подготовленной ещё в 2004 году, потому что хотим выразить свою точку зрения в этом вопросе, существенно отличающуюся от позиции авторов отмеченной работы, в которой рассматриваются итеративные шифры и их устойчивость к атакам линейного и дифференциального криптоанализа. Отмечается, что в теории эти нападения предполагают независимость от цикловых ключей шифров. Очень часто, однако, цикловые ключи вычисляются с помощью схем разворачивания ключей (ключевых расписаний) из короткого ключа в неслучайном режиме. С помощью экспериментов авторы показывают, что шифры со сложным ключевым графиком противостоят атакам линейного и дифференциального криптоанализа лучше, чем шифры с более простым ключевым графиком. Отмечается также известное в криптографической литературе положение, что с предположением независимых ключей вероятности дифференциалов и линейных оболочек могут быть смоделированы с помощью цепей Маркова и что для большинства таких шифров распределение вероятностей дифференциалов и линейных оболочек сходится к равномерному распределению после некоторого числа циклов. Представленные эксперименты с уменьшенными моделями шифра DES показывают, пишут авторы работы [1], что некоторые итеративные шифры с очень простым ключевым графиком никогда не достигают этого равномерного распределения. Кроме того, эксперименты показывают, что шифры с хорошо продуманным, сложным ключевым графиком достигают равномерного распределения быстрее (с использованием меньшего количества циклов), чем шифры с плохо разработанным ключевым графиком. В качестве побочного результата авторы отмечают, что существуют шифры, для которых дифференциал с наибольшей вероятностью для одного фиксированного ключа совпадает с дифференциалом с наибольшей вероятностью для любого другого ключа. Авторы считают, что это первый такой пример, приведенный в литературе. Имеются и другие публикации (например, [2, 3]), поддерживающие позицию авторов работы [1].

Цель данной статьи – ревизия изложенных выше результатов. Покажем, что как и в других наших работах [4, 5 и др.] показатели стойкости шифров к атакам линейного и дифференциального криптоанализа не зависят от схем разворачивания ключей. Кроме того, утверждение о том, что для любых ключевых графиков и большинства шифров, отнесенных к марковским, распределение вероятностей дифференциалов и линейных оболочек сходится к равномерному распределению после некоторого количества циклов, является неверным. Все шифры, как показано в [6, 7] являются марковскими и асимптотически приходят к показателям, свойственным случайным подстановкам. Наконец, покажем, что факт того, что существуют шифры, для которых дифференциал с наибольшей вероятностью для одного фиксированного ключа практически совпадает с дифференциалом с наибольшей вероятностью для любого другого ключа, является истиной для любого итеративного шифра. Более того, это свойство справедливо и для максимумов смещений линейных оболочек.

Эксперименты

Работа [1] строится на использовании уменьшенных версий шифров (8-битная, 10-битная, 12-битная). Но дело в том, что получить уменьшенную версию, повторяющую свойства большой, для шифра DES со слабым линейным преобразованием это нереализуемая

задача. Учесть нюансы, состоящие в том, что имеется слабость у третьего S-блока для дифференциального криптоанализа и слабость у 5-го S-блока для линейного криптоанализа в малой модели просто невозможно потому, что приходится иметь дело с шифром со значительно уменьшенным по размерам входным блоком данных, для которого переходы с особыми вероятностями, обнаруженными Э. Бихамом и А. Шамиром, а также М. Мацуи, как мы покажем, "тонут" в существенно более высоких значениях вероятностей переходов, свойственных малым моделям шифров.

Наконец, авторы скорее стремились подтвердить имеющиеся в литературе результаты и положения, а не проверить их объективность. Вот и получилось, что в этой работе представляются ожидаемые авторами результаты, которые, как мы покажем, оказались далёкими от реального состояния дел.

Мы в своих экспериментах сразу остановились на полной версии шифра DES. Повторили в экспериментах все пять вариантов схем разворачивания ключей, рассмотренных в работе [1], только переработали их для большой версии шифра.

Как и в [1] рассматривали поцикловые распределения максимумов полных дифференциалов, только строилась часть дифференциальной таблицы 64-битного шифра. Мы воспользовались нашей методикой анализа дифференциальных свойств больших моделей шифров в режиме их применения для зашифрования усечённых до 16-битных значений блоков данных, позволяющей построить эксперименты, находящиеся в рамках реализуемых вычислительных возможностей [8, 9].

Первая серия наших экспериментов выполнена с шифром DES в его оригинальном исполнении, т.е. была взята схема разворачивания ключей, полностью повторяющая её реализацию в самом стандарте.

В табл.1 представлены поцикловые значения максимумов полных дифференциалов (максимальных значений переходов таблиц XOR разностей) для шифра DES с различными вариантами использования "родной" схемы разворачивания ключей.

Таблица 1

Число циклов	"Родной" ключ	Независимые цикловые подключи	Слабый ключ	Нулевые подключи
1	65536	65536	65536	65536
2	65536	65536	65536	65536
3	211526	20736	8192	22528
4	388	400	334	5600
5	32	18	18	172
6	18	18	20	782
7	20	20	18	835
8	20	20	20	878
9	20	22	18	844
10	18	18	20	18
11	20	18	20	20
12	20	20	20	20
13	20	18	18	22
14	18	18	18	18
15	20	18	18	18
16	20	20	18	18

В первой колонке представлены значения дифференциалов при использовании в DES штатной схемы разворачивания ключей. Во второй колонке приведены данные для шифра, когда используется случайный набор цикловых подключей (схемы разворачивания ключей как таковой нет). В третьей колонке осуществляется зашифрование на слабом ключе: FEFEFE.... Видно, что в первых трёх случаях шифр DES после 5-ти 6-ти циклов зашифрова-

ния приходит к показателям случайной подстановки степени 2^{16} (становится случайной подстановкой). Слабый ключ (в шифре DES схема формирования цикловых подключей допускает ситуацию, когда во всех циклах алгоритма формируется один и тот же ключ) тоже не меняет общую ситуацию. Нулевые подключи в шифре DES затягивают переход к случайной подстановке до 10-ти циклов. Это просто означает, что алгоритм шифрования сам по себе не обладает хорошими перемешивающими свойствами.

В табл.2 представлены результаты второй серии экспериментов, где мы интересовались поцикловыми значениями максимумов смещений линейных оболочек шифра DES при различных вариантах использования схемы разворачивания ключей.

Таблица 2

Число циклов	"Родной" ключ	Независимые цикловые подключи	Слабый ключ	Нулевые подключи
1	32768	32768	32768	32768
2	32768	32768	32768	32768
3	20480	20480	20480	20480
4	2320	2952	3490	3206
5	810	845	840	783
6	870	803	807	821
7	805	815	859	791
8	860	839	824	802
9	823	809	848	802
10	779	839	816	835
11	803	773	828	828
12	802	789	817	854
13	782	799	829	831
14	835	814	811	804
15	878	876	852	799
16	844	832	811	816

В этом случае получается, что наличие или отсутствие ключей зашифрования не влияет на линейные свойства шифрующего преобразования. Во всех случаях шифры DES на пятом цикле зашифрования приходят к показателям случайной подстановки степени 2^{16} (становятся случайными подстановками).

Уже из этих результатов становится понятно, что в рамках наших экспериментов различные схемы разворачивания ключей не повлияют на дифференциальные и линейные свойства шифра. Но мы добросовестно повторили все последующие эксперименты работы [1].

Как и в работе [1], были использованы пять вариантов построения схем разворачивания ключей. Кратко напомним эти решения с учётом их модификации применительно к большому шифру DES.

В качестве входных данных для четырех названных основными ключевых графиков теперь уже рассматривается 96-битный ключ K, из которого формируется r 48-битных битных цикловых подключей K_i для $i = 1, ..., r$. Все четыре алгоритма берут выбранный пользовательский ключ и разделяют его на две 48-битные половины K^L и K^R.

Первый ключевой график строится следующим образом:

Key schedule 1:
Input: $K = K^L \mid K^R$
For i =1 **to** r/2 **do**
$K_{2i-1} = K^L$
$K_{2i} = K^R$
For $i = 0$ **to** r **do** $K_i = K_i$ XOR i.

Здесь цикловые подключи конструируются простым повторением отобранных пользователем ключевых половинок для каждого из циклов.

Хорошо известно, отмечают авторы работы [1], что такие ключевые графики оставляют шифр очень уязвимым для так называемых связанных ключевых атак [10, 11], а также слайд атак [12]. Тем не менее, это ключевое расписание, считают они, является слабым и в том смысле, что циклы шифра с четными номерами зависят только от одной ключевой половины, а циклы шифра с нечетными номерами зависят только от второй ключевой половины.

Чтобы избежать этой симметрии второй ключевой график использует ключевые половины в циклах в ином порядке:

Key schedule 2:
Input: $K = K^L \mid K^R$
For i =1 **to** r/4 **do**
$K_{4i-3} = K^L$
$K_{4i-2} = K^R$
$K_{4i-1} = K^R$
$K_{4i} = K^L$
For i =0 **to** r **do** $K_i = K_i$ XOR i

Как следует из алгоритма, к цикловым ключам добавляются цикловые константы. Первые два графика используют 48-битные половинки K непосредственно, то есть наименее значимый бит циклового ключа зависит только от наименее значимого бита двух половинок входного ключа.

Чтобы избежать таких свойств, третий график использует сдвиги (ротации) чтобы распространять влияние битов ключа K по всем позициям цикловых подключей:

Key schedule 3:
Input: $K = K^L \mid K^R$
$K_1 = K^L$
$K_2 = K^R$
K_3 = LeftShift(K^L, 24) + RightShift(K^R, 24)
K_4 = LeftShift(K^R, 24) + RightShift(K^L, 24)
For i = 5 **to** r **do** K_i = Rotate(K_{i-3},12)
For i =1 **to** r **do** $K_i = K_i$ XOR i

Leftshift принимает 24 младших бита на вход и сдвигает их на 24 позиции влево. *Right-Shift* принимает 24 старших бита на вход и сдвигает их на 24 позиции вправо. Как следствие, третий цикловой подключ K_3 зависит от 24 битов из K^L и 24 битов из K^R, в то время как четвертый K_4 цикловой подключ зависит от остальных 24 битов K^L и K^R. Оставшиеся цикловые ключи генерируются как сдвинутые версии предыдущих цикловых ключей. Чтобы избежать тривиальной симметрии и слабых ключей, используются упорядоченные цикловые константы (различные для всех цикловых подключей).

Четвертый график еще сложнее. Здесь ряд (серия) цикловых подключей TK_1, ..., TK_r генерируются аналогично предыдущему. Затем эти цикловые ключи используются в шифре, о котором идёт речь, чтобы создать (реальные) цикловые ключи для экспериментов. Шифр используется в режиме счетчика и результирующие шифртектовые половины являются исключительно упорядоченными, для генерации (реальных) цикловых подключей .K_1,..., K_r:

Key schedule 4:
Input: $K = K^L \mid K^R$
$TK_1 = K^L$
$TK_2 = K^R$
$TK_3 = K^L$ XOR K^R
For i = 4 **to** r **do** TK_i = Rotate(TK_{i-3},1)

For i =0 **to** r **do** $TK_i = TK_i$ XOR i
TK:= { TK_1,..., TK_r}
For i =1 **to** r **do**
$C = (C^L \mid C^R)$ = encrypt(i,T_K)
$K_i = C^L$ XOR C^R

Пятый ключевой график просто использует независимые цикловые ключи, то есть для тестирования шифра выбранный пользователем ключ в общей сложности имеет 48r бит. Это "ключевой график" уже рассмотрен в первой серии экспериментов.

Результаты оценки влияния четырех представленных выше основных ключевых графиков на дифференциальные и линейные показатели шифра DES иллюстрируют табл. 3 и 4.

Табл. 3 иллюстрирует результаты третьей серии экспериментов при использовании в шифре DES приведенных выше четырёх схем разворачивания ключей. В этой серии экспериментов изучались дифференциальные показатели схем зашифрования.

Таблица 3

Число циклов	Схема разворачивания 1	Схема разворачивания 2	Схема разворачивания 3	Схема разворачивания 4
1	65536	65536	65536	65536
2	36864	43008	43008	43008
3	12908	12350	25392	21128
4	302	132	114	118
5	18	18	20	18
6	20	18	20	18
7	20	20	20	18
8	18	18	20	20
9	20	18	18	18
10	18	20	18	18
11	20	20	18	20
12	18	18	20	20
13	20	20	20	20
14	20	20	18	18
15	20	20	18	20
16	20	20	20	20

Для всех перечисленных ключевых графиков перебор был реализован так, чтобы найти все дифференциалы и линейные оболочки для различного числа циклов. Для r-цикловой версии шифра и для каждого ключевого графика эксперименты проводились следующим образом:

Для каждого значения ключа были вычислены все r-цикловые дифференциалы и все r-цикловые линейные оболочки (корпуса). Корпус и дифференциал с наибольшей вероятностью по всем входам записывались. В наших экспериментах в отличие от работы [1] все расчёты выполнялись на одном из вариантов ключа зашифрования. Здесь уже учитывался опыт выполнения подобных исследований [4, 5], в соответствии с которым результаты, как для максимумов дифференциалов, так и для максимумов смещений практически не зависят от ключа зашифрования. Среднеквадратическое отклонение не превышает значения ±1,5 для максимумов дифференциалов и ± 35 для максимумов смещений.

Табл. 4 иллюстрирует результаты четвёртой серии экспериментов при использовании в шифре DES приведенных выше четырёх схем разворачивания ключей. В этой серии экспериментов изучались линейные показатели схем зашифрования.

Во всех рассмотренных случаях получается, что различные схемы разворачивания ключа на уровне оценки дифференциальных и линейных показателей 16-битных переходов для

шифра DES приводят к одним и тем же результатам. Через пять-шесть циклов все варианты шифров приходят к показателям случайной подстановки степени 2^{16}.

С другой стороны, известно, что большой шифр DES приходит к показателям случайной подстановки не через пять циклов, а гораздо позже. (Вспомним дифференциальную 13-цикловую характеристику для входной разности "1960", на которую построили атаку Э. Бихам и А. Шамир.)

Просто в 16-битном варианте построения дифференциальной характеристики, использованном в работе, выделить этот особый переход не представляется возможным. Максимум перехода при 13 циклах, который соответствует вероятности $2^{-47,2}$, равен значению $2^{16,8} = 114104,8$ (это для дифференциальной таблицы размером $2^{64}\times2^{64}$). Для фрагмента таблицы $2^{32}\times2^{32}$ ожидаемое значение максимума будет равно $\sqrt{114105} \approx 337,8$. а для фрагмента таблицы размером $2^{16}\times2^{16}$ значение максимума соответственно получается равным $\sqrt{338} \approx 18$, что на уровне ожидаемого значения максимума случайной подстановки степени 2^{16} для особенного перехода "1960" уже не заметишь.

Таблица 4

Число циклов	Схема разворачивания 1	Схема разворачивания 2	Схема разворачивания 3	Схема разворачивания 4
1	32768	32768	32768	32768
2	32768	32768	32768	32768
3	22528	14336	17664	20480
4	2744	4176	3464	2508
5	806	797	864	824
6	776	810	824	829
7	818	811	825	835
8	805	787	811	831
9	844	845	818	809
10	794	799	860	843
11	825	816	857	886
12	828	817	815	808
13	871	837	817	788
14	812	804	847	838
15	799	847	810	846
16	834	834	894	824

В этом видится один из недостатков использования малых моделей, который проявляется в нивелировании переходов, превышающих стандартные значения максимумов дифференциальной таблицы большого шифра множеством значений переходов, приходящихся на существенно уменьшенную её часть. В данном случае из всей таблицы размером $2^{64}\times2^{64}$ рассматривается только часть размером $2^{16}\times2^{16}$.

Ещё одно объяснение этого эффекта. Можно реализовать малую (16-битную) модель шифра DES с первыми тремя "родными" S-блоками, повторяющую особенности реализации большого шифра DES. Цикловая функция в этом случае строится так. Правая половинка из восьми бит входного блока данных дополняется расширением E до 12 битов, так что на входы трёх S-блоков цикловой функции поступают биты в таком порядке 12, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. На вход первого S-блока поступают 12, 1, 2, 3, 4, и 5-й биты, на вход второго S-блока поступают 4, 5, 6, 7, 8, и 9-й биты и на вход третьего S-блока поступают 8, 9, 10, 11, 12, и 1-й биты. В этом наборе из 12 битов повторяющимися являются 4 и 5-й биты, 8 и 9-й биты, 12 и 1-й биты (всего получается восемь различных битов входа). Далее идут, как и положено, S-блоки и P подстановка. С такой цикловой функцией можно реализовать переход 1960 и для малого шифра с вероятностью 1/234, свойственный "большому" DES.

Тогда для 16-битного шифра вероятность перехода 1/234 за первые два цикла приводит к значению перехода на выходе равному 280; вероятность 1/234 для первой и второй пары циклов даёт уже значение перехода 1,19, что значительно меньше двадцатки. В результате. получается, что и для малой модели уже после четырех циклов значение особого перехода "тонет" в значениях других переходов. Малая модель, как и рассмотренная выше большая для 16-битных переходов становится случайной подстановкой после 5-6-ти циклов независимо от схемы разворачивания ключей.

Тем более нельзя зафиксировать отмеченную выше особенность реализации шифра DES в уменьшенных до 8-10 битовых входов моделях, рассмотренных в работе [1]. Таким образом, в наших исследованиях мы полностью повторили эксперименты работы [1].

Вспомним теперь о большом шифре DES.

Мы нашли ещё две работы [14, 15], связанные с изучением возможностей реализации атак дифференциального криптоанализа на шифр DES. В работе [14] отмечено, что вероятность 1/234 является только средней вероятностью. Более того, наряду с входной разностью $\Phi = 19600000_x$ (в наших обозначениях это разность "1960") существует и входная разность $\Gamma = 1b600000_x$ с такой же средней вероятностью перехода. Эту возможность описывали Э. Бихам и А. Шамир в работе [16]. В этой работе, на которую есть ссылка и в работе [14], указано, что если шестой ключевой бит, используемый в S2, отличается от второго ключевого бита, используемого в S3, то вероятность для входа Φ увеличивается до 1/146, в то время как вероятность для входа Γ уменьшается до 1/585. Если же эти два ключевых бита равны, то результирующие вероятности меняются местами.

Авторы работы [14] назвали эти ключевые биты *критическими* для Φ и Γ. В своей атаке на DES [17] Бихам и Шамир использовали эти две характеристики, чтобы построить 13-цикловые характеристики, где шесть циклов имеют входной xor Φ или Γ. Вероятность, как утверждается, должна быть $(1/234)^6 \approx 2^{-47,22}$. Но в зависимости от значений шести пар критических ключевых битов вероятность для Φ будет варьироваться в пределах от $(1/146)^6 \approx 2^{-43,16}$ до $(1/585)^6 \approx 2^{-55,16}$ и, наоборот, для Γ.

И тут дело не в специально подобранной схеме разворачивания ключей. Э. Бихам и А. Шамир в своей работе полагали ключевые биты, воздействующие на S-блоки статистически независимы. Их методика вычисления вероятности двухцикловой характеристики обнуляющего типа основывалась на допущении, что после сложения расширенного входного полублока данных с цикловым подключом (биты которого в пределах подключа независимы) входы двух смежных (соседних) S-блоков также становятся "статически" независимыми [15]. Однако более тщательный анализ F функции показывает (это мы цитируем работу [15]), что использование в шифре DES сложения с подключом после E расширения приводит к тому, что условия "сшивки" S-блоков становятся зависимыми от ключевых битов, о чём говорится в работе [14]. Получается, что даже в оригинальной разработке DES при использовании "родной" схемы разворачивания ключей возможны семь вариантов вероятностей в указанном выше диапазоне, а каждое из предельных значений вероятностей возможно на 2^{50} ключей, т.е. на каждом 64-м ключе. Значение 2^{-47}, использованное Э. Бихамом, может быть получено как среднее от двух предельных значений:

$$(1/146)\cdot 1/2 + (1/585)\cdot 1/2 = 1/234.$$

При организации атаки нападающий не знает значения ключа зашифрования и вынужден ориентироваться на среднее значение характеристики, а это значение не зависит от значений цикловых подключей. Представляется, что этот же эффект буде наблюдаться и при иных схемах разворачивания ключей. Тем не менее, можно заключить, что для шифра DES его стойкость к атакам, по крайней мере дифференциального криптоанализа, зависит от схемы разворачивания ключей (от ключевого графика).

При любых вариантах схем разворачивания ключей шифр рано или поздно приходит к показателям случайной подстановки.

Так, если исходить из того, что для 13-ти циклов мы имеем наибольшую вероятность максимального перехода $2^{-47,22}$, то ещё одна дополнительная двухцикловая характеристика (15 циклов) приводит к значению максимального ожидаемого перехода 114104,8/234 = = 487,63, а для 17 циклов имеем значение перехода 487,63/234 = 2,08 – значение существенно меньшее максимума полного дифференциала случайной подстановки степени 2^{64} (это значение максимума близко к 68 [18]. На 16-ти циклах шифрования шифр DES становится случайной подстановкой (здесь ведём вычисления с дифференциальной характеристикой, а не с полным дифференциалом, который по значению перехода должен превосходить дифференциальную характеристику). Даже при использовании двухцикловой характеристики с вероятностью 1/146 (специально подобранные цикловые подключи) шифр DES на 16-ти циклах приобретает ожидаемое значение максимума дифференциального перехода равное 88, что всё равно очень близко к 68.

Таким образом, можно сделать вывод о том, что схемы разворачивания ключей (исключая специально подобранные варианты) для полного шифра DES никакой криптографической значимости (по отношению к показателям стойкости к атакам дифференциального криптоанализа) не имеют. Независимо от того, присутствует ли какая-либо схема разворачивания ключей в шифре или цикловые ключи имеют нулевые значения, шифр DES после шестнадцати циклов приходит к показателям случайной подстановки. Особые переходы, имеющиеся в шифре DES, на наш взгляд, не имеют криптографической ценности, так как являются принадлежностью только этого шифра. Атака на шифр DES строится на использовании укороченная дифференциальная характеристика с переходами обнуляющего типа (специфическими именно для шифра DES), когда шифр ещё не достиг установившегося (стационарного) значения максимума полного дифференциала.

Одновременно полученные результаты подтверждают практическую независимость установившихся законов распределения полных дифференциалов шифра и распределения смещений таблицы линейных аппроксимаций от ключей шифрования.

Если вспомнить теорему [13] о том, что с момента прихода шифра к стационарному состоянию дальнейшее наращивание числа циклов не меняет закона распределения полных дифференциалов (смещений ЛАТ) на его выходе, то становится понятным, что результирующее распределение полных дифференциалов, как и результирующее распределение смещений линейных оболочек, никогда не приходит к значению $p = 2^{-64}$.

Заметим далее, что имеющаяся в шифре DES особенность, позволяющая реализовать эффект накопления вероятностей на отдельных переходах, связана с возможностью реализации в шифре характеристик обнуляющего типа, когда ненулевая разность на входе преобразования переходит в нулевую разность на выходе (когда удаётся при формировании дифференциальных характеристик использовать переходы $0 \rightarrow 0$ без потери вероятностей). Условиями возникновения такой ситуации являются:

1) использование в шифре несимметричных S-блоков, допускающих переходы входной ненулевой разности в нулевую выходную;

2) применение петлевой схемы формирования цикловых переходов, при которой удаётся реализовать попеременное чередование активных и пассивных циклов;

Очевидно, что эти условия не выполняются для шифров с квадратными S-блоками (для SPN шифров и ряда известных Фейстель подобных шифров: Камелия, ГОСТ 28147-89 и др.). Шифр DES выступает здесь как заметное исключение.

Выводы

По результатам экспериментов все схемы разворачивания ключей для шифра DES приводят к одному и тому же результату. Это значит, что, по крайней мере, на уровне 16-битных дифференциальных показателей схемы разворачивания ключей для шифра DES не оказывают существенного влияния на стойкость к атакам дифференциального и линейного криптоа-

нализа. Имеющиеся особые переходы в шифре DES в той или иной мере будут характерны для схем разворачивания ключей всех конструкций.

Показатели стойкости шифра зависят не от схем разворачивания ключей, а от значений используемых ключей, от присутствия в цикловых подключах критических битов. Среднее значение вероятностей дифференциальных характеристик, по-видимому, будет одним и тем же для разных схем разворачивания ключей.

Все итеративные шифры, как следует из развиваемой в [13] методологии оценки стойкости в БСШ к атакам дифференциального и линейного криптоанализа, после небольшого начального числа циклов зашифрования (в наших экспериментах для DES после 5-6, а для полного DES после 16 циклов) приходят к стационарным состояниям, свойственным случайным подстановкам соответствующих степеней, которые сохраняются при наращивании числа циклов, и, следовательно, предельные распределения не являются равномерными.

Список литературы: 1. *Lars R. Knudsen1 and John E. Mathiassen.* On the Role of Key Schedules in Attacks on Iterated Ciphers. P. Samarati et al. (Eds.): ESORICS 2004, LNCS 3193, pp. 322–334, 2004. Springer-Verlag Berlin Heidelberg 2004. 2. *Uri Blumenthal and Steven M. Bellovin,* A better Key Schedule for DES-like ciphers. Proceedings of Pragocrypt'96 30 September – 3 October 1996. 3. *Лепеха, А.Н.* Сравнительный анализ схем разворачивания ключей блочных симметричных шифров / А.Н. Лепеха // Радиотехника. – 2005. – Вып. 141. – С. 64 -69. 4. *Долгов, В.И.* Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс / В.И. Долгов, А.А. Кузнецов, С.А. Исаев // Электронное моделирование. – 2011.– Т 33, № 6. – С. 81-99. 5. *Кузнецов, А.А.* Линейные свойства блочных симметричных шифров, представленных на украинский конкурс / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. – 2011. – Т.10. №2 – С. 135-140. 6. *Лисицкая, И.В.* блочные симметричные шифры и марковские процессы / И.В. Лисицкая // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2 – С. 137-143. 7. *Лисицкая, И.В.* Оценки максимальных значений дифференциалов и линейных корпусов Марковских шифров / И.В. Лисицкая., В.И. Долгов, А.А. Настенко // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2 – С. 144-151. 8. *Лисицкая И.В.* Большие шифры – случайные подстановки / И.В. Лисицкая, А.А. Настенко // Радиотехника. – 2011. – Вып. 166. – С. 50-55. 9. *Лисицкая, И.В.* Дифференциальные свойства шифра FOX / И.В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. – 2011. – Т. 10, № 2. – С. 122-126. 10. *Biham, E.* New types of cryptanalytic attacks using related keys. In T. Helleseth, editor, Advances in Cryptology: EUROCRYPT'93, Lecture Notes in Computer Science 765, pages 398–409. Springer Verlag, 1993. 11. *Knudsen, L.R.* Cryptanalysis of LOKI'91. In J. Seberry and Y. Zheng, editors, Advances in Cryptology, AusCrypt 92, Lecture Notes in Computer Science 718, pages 196–208. Springer Verlag, 1993. 12. *Biryukov, A. and Wagner, D.* Slide attacks. In L. R. Knudsen, editor, Fast Software Encryption, Sixth International Workshop, Rome, Italy, March 1999, Lecture Notes in Computer Science 1636, pages 245–259. Springer Verlag, 1999. 13. *Лисицкая,И.В.* Методология оценки стойкости блочных симметричных шифров / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123-133. 14. *Knudsen, L.R.* Iterative characteristics of DES and s^2-DES, Advances in Cryptology, Proc. Crypto '92, LNCS 740, E. F. Brickell, Ed., Springer-Verlag, 1993, pp. 497-511. 15. *Головашич, С.А.* Ключевые группы в атаках дифференциального криптоанализа DES-подобных шифров / С.А. Головашич // Радиотехника.– 2000. – Вып. 114. – С. 57-62. 16. *Eli Biham, Adi Shamir.* Differential Cryptanalys is of DES- like Cryptosystems. Journal of Cryptology, Vol. 4 No. 1 1991. 17. *Eli Biham, Adi Shamir.* Differential Cryptanalysis of the full 16- round DES. Technical Report # 708, Technion – Israel Institute of Technology. 18. *Олейников, Р.В.* Дифференциальные свойства подстановок / Р.В. Олейников, О.И. Олешко, К.Е. Лисицкий, А.Д. Тевяшев // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326-333.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 25.09.2012