УДК 003.26

Лисицкая И. В.[1], Лисицкий К. Е.[2], Родинко М. Ю.[3], Головко И. А.[3], Жариков И. И.[3], Корниенко М. А.[3], Кулеба М. В.[3]

[1]Д-р техн. наук, профессор, профессор кафедры БИСТ Харьковского национального университета им. В.Н. Каразина, Харьков, Украина
[2]Студент Харьковского национального университета имени В. Н. Каразина
[3]Студенты Харьковского национального университета радиоэлектроники, Харьков, Украина

ЭКСПЕРИМЕНТАЛЬНЫЕ ДАННЫЕ ПО ОПРЕДЕЛЕНИЮ ДИНАМИЧЕСКИХ ПОКАЗАТЕЛЕЙ ПРИХОДА БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ К СОСТОЯНИЮ СЛУЧАЙНОЙ ПОДСТАНОВКИ

Актуальность. Объектом исследований данной работы являются процессы прихода блочных симметричных шифров к состоянию случайной подстановки.

Цель работы. Уточнение с помощью вычислительных экспериментов значений динамических показателей прихода ряда современных шифров к состоянию случайной подстановки, которые могут стать важными при сравнительной оценке их эффективности.

Метод. Методика выполнения экспериментов состоит при определении дифференциальных показателей в активизации шифров (программных моделей) наборами входных разностей и последующего определения минимального количества S-блоков активизируемых на первых циклах зашифрования, позволяющих получить значение дифференциальной вероятности соответствующее показателю стойкости рассматриваемого шифра. При определении линейных показателей перебираются ненулевые маски входов в S-блоки и ненулевые маски их выходов.

При этом на входе шифра активизируется один байт входного блока данных, причем выбирается байт, который активизирует минимальное число S-блоков первого цикла. Здесь под активным байтом (S-блоком) понимается байт (S-блок), с помощью которого для пары входов в шифр (в S-блок) формируется ненулевая входная (выходная) разность. Затем в режиме зашифрования полным перебором всех 256 битных однобайтовых разностей входа шифра определяется минимальное число активизируемых S-блоков на каждом из циклов, которые пересчитываются в числа циклов зашифрования, необходимых для прихода шифра к случайной подстановке. Близкая по смыслу процедура может быть выполнена и при анализе линейных показателей с использованием входных и выходных масок.

Результаты. Полученные результаты свидетельствуют о том, что конструкции первых цикловых преобразований блочных симметричных шифров играют важную роль в обеспечении динамических показателей прихода шифров к состоянию случайной подстановки, и существенно влияют на значения числа циклов, необходимых для обеспечения запаса их стойкости. Все рассмотренные (известные) конструкции современных 128-ми битных блочных симметричных шифров, за исключением шифров IDEA NXT, Калина, Мухомор и белорусского шифра, обеспечивают динамические показатели прихода к состоянию случайной подстановки превышающие три-четыре цикла.

Шифр Rijndael оказывается далеко не в лидерах по рассматриваемому показателю (для прихода к состоянию случайной подстановки ему необходимо 4-ре цикла).

Выводы. В работе решена задача уточнения и подтверждения с помощью вычислительных экспериментов эффективности новой методики оценки динамических показателей прихода шифров к состоянию случайной подстановки.

Научная новизна результатов статьи состоит в том, что впервые получены обоснованные объективные данные для значений числа циклов прихода к состоянию случайной подстановки ряда современных шифров.

Практическая значимость предлагаемой методики и представленных в работе результатов состоит в их конструктивизме. Они позволяют выполнить обоснование числа циклов шифрующих преобразований, которые обеспечивают достижение предельного уровня стойкости шифров.

Ключевые слова: блочный симметричный шифр, динамические показатели, состояние случайной подстановки, стойкость к атакам дифференциального и линейного криптоанализа, активные S-блоки.

НОМЕНКЛАТУРА

XOR – побитовая сумма по модулю 2;

AMDP – среднее значение максимума дифференциальной вероятности;

ДХ – дифференциальная характеристика;

S-блок – табличная подстановка;

$DP_{\max}^{\pi}$ – максимальное значение дифференциального перехода таблицы подстановки π;

π – нелинейное преобразование (S-блок);

$k_{\min}$ – минимальное число активизируемых S-блоков, необходимых для прихода шифра к состоянию случайной подстановки;

МДР – порождающая матрица кода с минимальным (допустимым) кодовым расстоянием;

M-64 – функция усложнения шифра Мухомор-128;

SL-преобразование – 4-х байтовое Rijndael-подобное линейное преобразование цикловой функции;

l_k – размер ключа;

F-функция – элемент циклового преобразования шифра Camellia;

ШУП-1 – шифр с управляемыми подстановками первой версии.

ВВЕДЕНИЕ

Эта работа выполнена в развитие новой методологии оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, предложенной Лисицкой И. В. [1, 2 и др.]. Основным содержанием этой методологии является положение, в соответствии с которым практически все блочные

DOI 10.15588/1607-3274-2017-1-15

симметричные шифры через небольшое число циклов зашифрования становятся случайными подстановками (максимумы дифференциальных и линейных вероятностей шифров принимают установившиеся значения, характерные для случайных подстановок).

Объектом исследований данной работы являются процессы прихода блочных симметричных шифров к состоянию случайной подстановки.

В рамках этой работы во всех случаях независимо от способа введения в шифры ключевой информации мы будем интересоваться прохождением через шифры XOR разностей, поскольку все шифры асимптотически по отношению к XOR разностям ведут себя одинаково (ведут себя как случайные подстановки). Мы имеем здесь возможность привести все шифры к единой шкале оценок стойкости к атакам дифференциального криптоанализа.

Предметом исследований являются дифференциальные показатели прихода блочных симметричных шифров к состоянию случайной подстановки.

Развиваемая методика ориентирована на использование полномасштабных алгоритмов шифрования. Подход позволяет выполнить более точное сравнение шифров по стойкости, так как при общих одинаковых максимальных значениях дифференциальных (и линейных) вероятностей полноцикловых версий шифров их можно сравнивать по числу циклов необходимых для прихода шифров к состояниям случайной подстановки. Это реальный путь выполнения сравнения шифров по эффективности. Тот шифр считается более эффективным, который приходит к состоянию случайной подстановки за меньшее число циклов.

Целью данной работы является уточнение с помощью вычислительных экспериментов значений динамических показателей прихода ряда современных шифров к состоянию случайной подстановки, которые могут стать важными при сравнительной оценке их по эффективности.

1 ПОСТАНОВКА ЗАДАЧИ

В работах [3, 4, 5] уже изложены теоретические и практические соображения по формированию оценок динамических показателей прихода шифров к состоянию случайной подстановки. Здесь и далее под динамическими показателями прихода шифра к состоянию случайной подстановки понимается минимальное число циклов зашифрования, после которых шифр становится случайной подстановкой (приходит к стационарным значениям максимумов дифференциальных и линейных вероятностей, характерных для случайных подстановок). В этой работе ставится задача определения теперь уже экспериментальным путем минимального количества S-блоков активизируемых на первых циклах шифрования, обеспечивающих достижение теоретических (расчетных) показателей стойкости (значений максимумов дифференциальных и линейных вероятностей), на основе которых можно оценить минимально допустимые числа циклов зашифрования, после которых шифры становятся случайными подстановками.

2 ЛИТЕРАТУРНЫЙ ОБЗОР

В соответствии с развиваемой в работах [1, 2] новой методологией оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа эти показатели определяются асимптотическими значениями максимумов дифференциальных и линейных вероятностей шифров, при этом полагается, что все шифры после небольшого числа первых циклов зашифрования становятся случайными подстановками. В противоположность существующей точке зрения [6–14 и мн. др.], связывающей показатели стойкости шифров с дифференциальными и линейными показателями входящих в цикловые функции шифров S-блоков, в новой методологии [1, 2] утверждается, что криптографические показатели S-блоков не влияют на стойкость шифров к атакам дифференциального и линейного криптоанализа. Они влияют лишь на динамику прихода шифров к состоянию случайной подстановки, т.е. на число циклов шифрования, после которого максимальные значения дифференциальной и линейной вероятностей шифров принимают стационарные значения, свойственные случайной подстановке, и это число циклов для современных шифров может отличаться от шифров со случайно взятыми S-блоками лишь одним циклом. В то же время существуют и шифры, где S-блоки вообще не влияют на динамику прихода шифров к состоянию случайной подстановки. В этой связи возникает интерес к изучению динамических показателей прихода шифров к состоянию случайной подстановки, так как на их основе появляется дополнительная возможность для сравнения шифров по эффективности шифрующих преобразований.

3 МАТЕРИАЛЫ И МЕТОДЫ

В этой работе внимание сосредотачивается на самом процессе (динамике) перехода шифров к состоянию случайных подстановок. В этом направлении уже был выполнен ряд работ. Так, в уже отмеченных выше работах [3, 4, 5] изложена методика определения динамических показателей прихода шифров к состоянию случайной подстановки, в частности, на основе этой методики определяются оценки ожидаемых показателей прихода к состоянию случайной подстановки ряда современных шифров исходя из интуитивных соображений. Эта методика строится на положении, в соответствии с которым результирующие значения дифференциальных и линейных вероятностей шифров формируются на основе произведения соответствующих переходных вероятностей активных S-блоков, входящих в их характеристики. Справедливость этого подхода в теоретическом отношении связана с предположением о независимости цикловых подключей шифров, На самом деле механизм случайного перемешивания выходов S-блоков в реальных конструкциях цикловых преобразований работает и без ключевых добавок. Как показали многочисленные эксперименты показатели случайности шифров как с реальными подключами, так и с подключами с нулевыми значениями (их отсутствии) совпадают [см., например, 15].

Активными S-блоками для дифференциальных показателей здесь и далее названы S-блоки с ненулевыми входными и выходными разностями. Активными S-блоками для линейных показателей названы S-блоки с ненулевыми выходами для ненулевых масок на их входах и выходах.

Развитый в работах [3, 4, 5] подход примечателен тем, что в нем используются достаточно точные значения показателей стойкости шифров к атакам дифференциального и линейного криптоанализа, которые в соответствии с новой методологией могут быть определены из формул для законов распределения переходов таблиц дифференциальных разностей и законов распределения смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степеней, установленных в работах [16–18].

В этой работе, как отмечено выше, ставится задача экспериментального исследования влияния механизмов активизации S-блоков цикловых функций шифров на процессы их прихода к состоянию случайной подстановки. В числе рассмотренных ряд современных шифров Rijndael, IDEA NXT, Мухомор, Белорусский шифр, Калина-2, Camellia и др.

Для выполнения экспериментов используются программные модели шифров, так как необходимо иметь возможность подключаться к выходам S-блоков цикловых функций и измерять их байтовые значения.

Методика выполнения экспериментов состоит при определении дифференциальных показателей в активизации шифров (программных моделей) наборами входных разностей и последующего определения минимального количества S-блоков активизируемых на первых циклах зашифрования, позволяющего получить значение дифференциальной вероятности соответствующее показателю стойкости шифра. При определении линейных показателей перебираются ненулевые маски входов в S-блоки и ненулевые маски их выходов.

При этом на входе шифра активизируется один байт входного блока данных, причем выбирается байт, который активизирует минимальное число S-блоков первого цикла. Здесь, как уже было отмечено выше, под активным байтом (S-блоком) понимается байт (S-блок), с помощью которого для пары входов в шифр (в S-блок) формируется ненулевая входная (выходная) разность. Затем в режиме зашифрования полным перебором всех 256 битных однобайтовых разностей входа в шифр определяется минимальное число активизируемых S-блоков на каждом цикле, которые пересчитываются в число циклов зашифрования, необходимых для прихода шифра к случайной подстановке. Близкая по смыслу процедура может быть выполнена и при анализе линейных показателей с использованием входных и выходных масок.

4 ЭКСПЕРИМЕНТЫ

Шифр Rijndael [19]**.** Для шифров, таких как Rijndael и ряда других сравнительно легко определить минимальное число активных S-блоков для прихода шифра к состоянию случайной подстановки и без вычислительных экспериментов. Мы, тем не менее, приводим здесь и динамические показатели шифра Rijndael, полученные экспериментальным путем. Эти результаты иллюстрирует табл. 1. В этой таблице приведены числа активизируемых S-блоков на соответствующих циклах зашифрования при активизации одного байта входа в шифр.

Эти же результаты следуют и из соображений, представленных в работах [3, 4, 5]. По приведенным данным шифр Rijndael приходит к состоянию случайной подстановки по дифференциальным показателям за три цикла (а по линейным за четыре).

Шифры семейства IDEA NXT [20]. Шифр IDEA NXT, на наш взгляд можно рассматривать в виде развитии стратегии широкого следа по пути увеличения числа активизируемых S-блоков цикловой функции. В шифрах IDEA NXT используется удвоенное (два слоя) число S-блоков функций усложнения, в результате чего минимальное число активизируемых S-блоков первого цикла получается равным 5-ти для 32-х битной функции усложнения и 9-ти для 64-х битной функции усложнения. По-видимому, основная роль схемы Lai-Massey – это получить за счет внешнего контура преобразования (схемы Lai-Massey) эффект удвоение числа активизируемых S-блоков циклового преобразования. Но тогда для 64-х битного шифра ожидаемое число активных S-блоков на первом цикле будет равным 10, а для 128-ми битного шифра равным 18-ти. На втором цикле для 128-ми битного шифра добавляется с учетом удвоения еще 32 активных S-блока. В результате шифр IDEA NXT-128 становится случайной подстановкой на втором цикле.

Здесь, однако, могут быть переходы с ненулевыми вероятностями в виде, например, такой последовательности активных S-блоков по их числам 9 = 2+7, 9 = 7+2, и на двух циклах (для 128-ми битного входа в шифр) здесь следует ожидать (с учетом удвоения) минимальное число 36-ть активных S-блоков. Но и в этом случае шифр становится случайной подстановкой после двух циклов. Вероятность получить такую характеристику равна 2^{-56}.

Это позволяет шифр IDEA NXT отнести к числу решений более эффективных, чем шифр Rijndael. Для подтверждения этого факта мы ниже приводим результаты экспериментов, выполненных практически в одних и тех же условиях, по определению поцикловых значений полных дифференциалов для 128-битных версий шифров FOX и Rijndael, заимствованные из работы [1]. Они представлены в табл. 2 и табл. 3.

Таблица 1 – Распределение числа активных S-блоков на первых циклах шифрования при активизации одного байта входа шифра Rijndael (65280 значений ненулевых разностей)

Число активных S-блоков	Число ненулевых однобайтовых разностей			
	1-й цикл	2-й цикл	3-й цикл	4-й цикл
0	0	0	0	0
1	65280	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	65280	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	1
14	0	0	0	119
15	0	0	0	3883
16	0	0	65280	61275

Таблица 2 – Поцикловые значения максимумов полных дифференциалов для 128-битной версии шифра FOX (для подсчета разностей во внимание принимаются отдельные 16 бит блоков данных)

Количество циклов	Биты 64..79 шифртекстов		Биты 80..95 шифртекстов		Биты 96..111 шифртекстов		Биты 112..127 шифртекстов	
	Максимум ДХ	Число максимумов	Максимум ДХ	Число максимумов	Максимум ДХ	Число максимумов	Максимум ДХ	Число максимумов
1	32	1	38	1	32	1	38	1
2	18	10	20	1	20	1	18	11
3	18	14	22	1	20	1	18	10
4	18	10	22	1	18	20	22	1
5	18	10	18	19	20	1	18	16
6	18	15	18	14	18	13	18	15
7	20	1	20	1	20	1	20	2
8	20	1	18	18	20	1	18	17
9	18	13	20	1	18	20	20	2
10	18	12	18	17	20	3	20	1
11	20	1	20	1	20	1	20	1

Таблица 3 – Поцикловые значения максимумов полных дифференциалов при активизации шифра Rijndael 16-битными блоками разностей

Число циклов r	Значение максимума полного дифференциала	Среднеквадратическое отклонение
1	1024	0
2	3652,26	± 630,312
3	19,0666	± 1,436
4	19,0666	± 0,99777
5	18,8666	± 1,23108
6	19,1332	± 0,99106
7	19,2666	± 1,0934
8	19,1332	± 1,431394
9	19,0666	± 1,23648
10	19,3333	± 1,2995
11	19,4	± 1,474222
12	18,8666	± 0,991072
13	18,8666	± 0,991072
14	18,9332	± 1,123486

В первом случае приводятся результаты оценки максимальных значений полных дифференциалов для 128-битной версии шифра FOX (с усечением шифруемых блоков (разностей) до 16-битного размера). В экспериментах рассматривались различные варианты входных 16-битных разностей. Во второй серии экспериментов использовался шифр Rijndael. В процессе экспериментов осуществлялось зашифрование 16-битных блоков данных на 30 случайно выбранных ключах. Затем полученные результаты усреднялись по этому множеству ключей (вычислялись, как определено в работе [1], AMDP – средние значения максимумов дифференциальных вероятностей).

Из представленных результатов видно, что большой шифр Rijndael уже с третьего цикла шифрования приходит к установившемуся значению максимума полного дифференциала, повторяющему соответствующее значение равное 18–20-ти, свойственное случайной подстановке степени 16-ть. Также видно, что это асимптотическое значение практически не зависит от используемых ключей зашифрования (среднеквадратическое отклонение не превышает 1,5). В то же время шифр FOX во всех случаях становится случайной подстановкой уже на втором цикле (FOX выигрывает у Rijndael-я по дифференциальным показателям один цикл). Это же следует и из результатов экспериментов по определению законов распределения числа активных S-блоков на первых циклах зашифрования 128-ми битного шифра IDEA NXT, представленных в табл. 4. Разработчики шифра этого не чувствуют и выбирают запас стойкости превышающий число циклов прихода шифра к состоянию случайной подстановки в шестеро (12-ть циклов).

Если же считать, что за счет внешнего контура преобразования (схемы Lai-Massey) происходит удвоение числа активных S-блоков цикловой функции, то 128-ми битная версия шифра приходит к состоянию случайной подстановки за два цикла. Отмеченное позволяет шифр IDEA NXT отнести к числу решений более эффективных, чем шифр Rijndael (для S-блоков этого шифра $DP^{\pi}_{\max} = 2^{-4} \rightarrow k_{\min}, = 30$, $LP^{\pi}_{\max} = 2^{-4}$ $k_{\min} = 40$ [3, 4]).

Таблица 4 – Числа активных S-блоков на первых циклах шифрования при активизации разностями одного байта входа шифра IDEA NXT (функции f64)

Число активных S-блоков	1-й цикл	2-й цикл	3-й цикл
0	0	0	0
1		0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	100	0	0
10	0	0	0
11	0	0	0
12	0	0,000784	0,000392
13	0	0,002353	0,003529
14	0	0,270196	0,169412
15	0	7,479216	5,896078
16	0	92,24745	93,93058

Шифр Мухомор [21]. Этот шифр тоже использует внешний контур зашифрования в виде схемы Lai-Massey. Вместе с тем, как отмечают некоторые исследователи, несмотря на внешние высокие показатели безопасности шифров этой серии, схеме Lai-Massey присуща слабость, которая заключаются в том, что она допускают переходы разностей на входах циклов в те же разности на их выходах, что приводит к возможности отключения (прохода без потери вероятности) половины циклов шифрования.

Мы здесь приведем для иллюстрации соображения, высказанные д.т.н. Олейниковым Р. В. Он приводит пример варианта характеристики для функции усложнения M-64, у которой совпадают входная и выходная разности, проиллюстрированный на рис. 1. и рис. 2. Конкретные значения, отмечает он, естественно, зависят от S-блоков и МДР-матрицы. В его примере выбран вариант более простой, чтобы без пересчета на компьютере был понятен принцип.

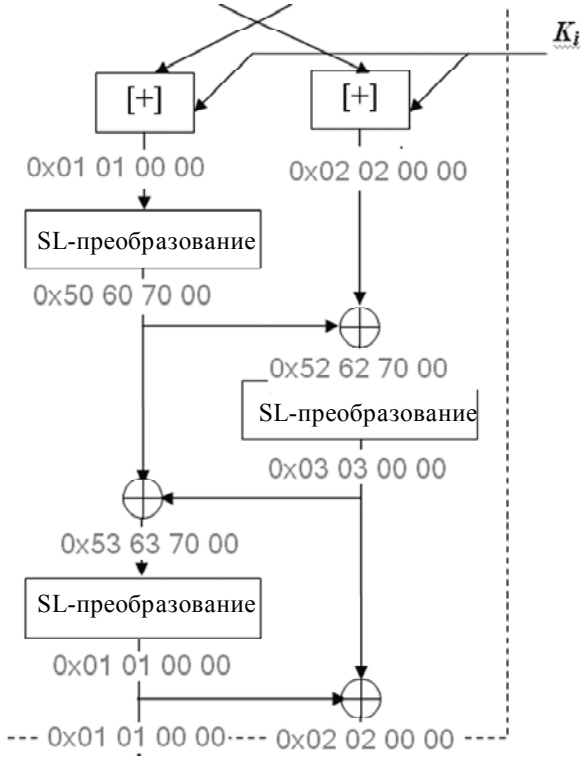

Рисунок 1 – Пример для функции усложнения M-64

Рисунок 2 – Проход МДР преобразования

Значения, для которых характеристика будет выполняться для S-блоков и МДР-матрицы из спецификации, можно подбирать на компьютере. Ключевой сумматор здесь считается XOR-ом. Как строить характеристики для модульного сумматора – отдельный вопрос, но тоже решаемый.

На входе M-64 – разность вида 01 01 00 00 02 02 00 00 в шестнадцатеричном виде. На выходе – то же самое значение. Почему на SL-преобразовании возможно получение перехода 01 01 00 00 в 50 60 70 00 (и других аналогичных)? Потому что для коэффициента ветвления 5-ть МДР матрица для двух активных байтов входа должна формировать три активных байта выхода.

Аналогично получаются переход разностей 52 62 70 00 в 03 03 00 00.

Итог: построение характеристики для M-64, у которой входная разность совпадает с выходной, с точки зрения выбора подходящих переходов не представляет сложности. Однако, как показал наш анализ, такие характеристики строятся из случайных переходов, среди которых попадаются невозможные, или весьма маловероятные. В многочисленных экспериментах по определению законов распределения переходов XOR таблиц 16-ти битных шифрующих преобразований и 32-ух битных в режиме активизации их 16-ти битными входами таких нетривиальных характеристик мы не обнаружили. Во всех случаях фиксировался максимум дифференциальной вероятности характерный для случайной подстановки 16-той степени. В результате отмеченный недостаток, на наш взгляд не дискредитирует шифр Мухомор.

Приведем показатели активизации S-блоков шифра Мухомор. Их иллюстрирует табл. 5. Очевидно, что минимальное число активных S-блоков получается при активизации правого SL преобразования в линейке SL преобразований первого слоя. Но запуск 32-ух битного входа этого SL преобразования осуществляется побитовой суммой по модулю два (разность по модулю два) первого и второго подблоков данных на входе цикла (см. описание шифра Мухомор [9]). Это значит, что один активный байт входа в правое SL преобразование первого слоя может быть сформирован на основе либо разности одного из подблоков (первого или второго), либо на основе разности, составленной из первого и второго подблоков входа. В соответствии с описанием шифра каж-

Таблица 5 – Распределение минимального числа активных S-блоков (в %) на первых циклах шифрования шифра Мухомор (для функции усложнения M-64)

Число активных S-блоков	1-й цикл	2-й цикл	3-й цикл
0	0	0	0
1		0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	100	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	0	0	0
12	0	100	100

дое из 32-ух битных входных значений функции М-64 складывается по модулю 2^{32} с соответствующей 32-ух битной половинкой циклового подключа. Но существует возможность выбрать активизируемые байты входа так, чтобы операции переноса разрядов при сложении половинок входного блока данных с половинками циклового подключа не приводила бы к увеличению числа активизируемых S-блоков (например, самый правый или самый левый байты входного блока данных). В результате будет активизироваться минимум один байт входа второго SL преобразования. Этот байт входа будет активизировать один S-блок этого SL преобразований и затем еще 4-ре S-блока второго слоя SL преобразований (очередного SL преобразования). Итого на первом цикле с большой вероятностью будет активизироваться минимум 5-ть S-блоков, а на втором все 12-ть S-блоков. За два цикла становятся активными 17-ть S-блоков функции усложнения М-64, а с учетом удвоения числа активных S-блоков схемой Lai-Massey шифр Мухомор приходит к состоянию случайной подстановки с запасом за два цикла.

Мы здесь приведем для иллюстрации результаты определения поцикловых значений максимумов переходов таблиц полных дифференциалов для полной версии шифра Мухомор в режиме его инициализации 16-битными разностями, выполненными в соответствии с методикой работы [1].

Результаты экспериментов иллюстрирует табл. 6, заимствованная из этой же работы. Здесь приводятся дифференциальные показатели сразу для трех шифров, представленных на украинский конкурс. Видно, что шифр Мухомор при активизации его 16-битными разностями приходит к показателям 16-битной случайной подстановки уже на первом цикле.

Блочный шифр из белорусского стандарта. Мы здесь сначала приведем краткое описание этого шифра, так как он относится к не так давно принятым стандартам и имеет оригинальную конструкцию [22].

Шифр построен на восьмикратном использовании одной и той же цикловой функции, приведенной на рис. 3. В каждом цикле шифра, как следует из рис. 3, используется 28-мь S-блоков.

Таблица 6 – Поцикловые значения максимумов переходов таблиц полных дифференциалов для полных версий украинских шифров при 16-битных разностях входа

Число циклов	Калина	ADE	Мухомор
1	19,47	65536	19,13
2	19,0	20	18,8
3	19,13	20	19,4
4	19,2	18	19,13
5	19.27	18	19,07
6	18,87	20	19,6
7	19,47	20	19,27
8	19,2	18	19,13
9	19,0	18	19,13
10	19,33	18	19,276

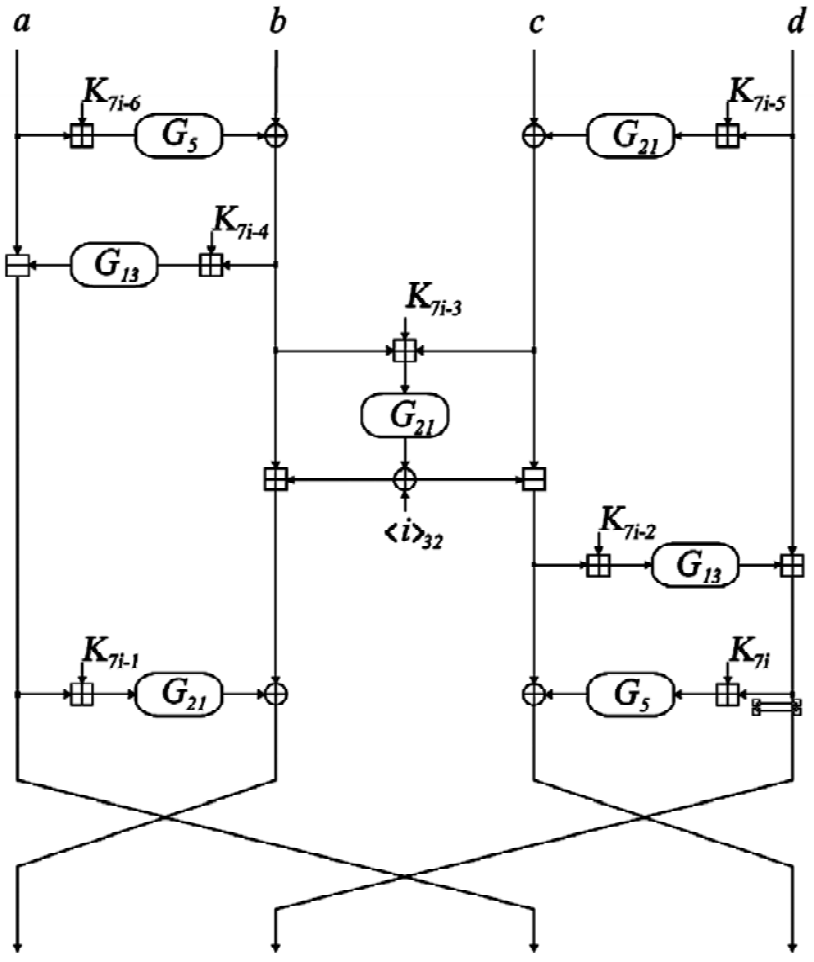

Рисунок 3 – Вычисления на *i*-м цикле зашифрования белорусского стандарта

Приведем расшифровку обозначений, использованных на этом рисунке [10]:

$\boxplus$ – сумматор по модулю 2^{32};

$\oplus$ – сумматор по модулю 2 (XOR);

$\boxminus$ – блок вычисления разности входных 32-битных слов по модулю 2^{32};

($u \boxminus \nu$ для u, $\nu \in \{0, 1\}^{8n}$ слово $w \in \{0, 1\}^{8n}$ такое, что $u = \nu \boxplus w$);

$<i>_{32}$ обозначает представление числа циклов i в двоичном виде (в виде 32-ух битного слова);

a, b, c, d – переменные со значениями из диапазона $\{0,1\}^{32}$.

Преобразование G_r (r = 5,13,21). Преобразование G_r: $\{0,1\}^{32} \to \{0,1\}^{32}$ ставит в соответствие 32-х битному слову на своем входе $u = u_1||u_2||u_3||u_4$, $u_i \in \{0, 1\}^8$ слово $G_r(u) = \mathrm{RotHi}^r\,(H(u_1)||H(u_2)||H(u_3)||H(u_4))$ на выходе, что в соответствии с обозначениями работы [22] отвечает представлению входного 32-х битного слова в виде 4-ех последовательных байтов, выполнению над каждым байтом операции нелинейного преобразования (подстановки) H и дальнейшего циклического сдвига объединения (конкатенации) – байтов с выходов подстановок на r = 5, 13 или 21 бит налево.

Входными данными алгоритмов зашифрования и расшифрования являются 128-битные блоки данных $X \in \{0,1\}^{128}$ и 128-битный, 192-битный или 256-битный ключи.

Табл. 7 иллюстрирует распределение числа активных S-блоков по циклам для шифра из белорусского стандарта (активизировался самый правый байт входа). В экспериментах в самом худшем маловероятном случае на первом цикле активизируется 7-мь S-блоков, а на втором 25-ть S-блоков из 28-ми возможных. Это значит, что на двух циклах при 31-ом активном S-блоке входа белорусский шифр становится случайной подстановкой при любых (случайных) S-блоках [3]. Во всех экспериментах использовались случайно взятые цикловые подключи.

Шифра Калина-2. В табл. 8 представлена картина активизации S-блоков трех первых циклов шифра Калина-2 [23]. Рассматривались ненулевые разности для самого левого и самого правого байта входного блока данных. И в этом случае использовались случайно сгенерированные цикловые подключи. Результаты для самого левого и самого правого байта входного блока данных получились идентичными. Представленные результаты

Таблица 8 – Распределение числа активных S-блоков на первых циклах (в %) при активизации одного байта входа шифра Калина-2

Число активных S-блоков	Число ненулевых однобайтовых разностей в процентах			
	1-й цикл	2-й цикл	3-й цикл, Key 1	3-й цикл, Key 2
0	0	0	0	0
1	100	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	100	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0,000392
13	0	0	0,002745	0,005490
14	0	0	0,183137	0,169020
15	0	0	5,818431	5,936078
16	0	0	93,995686	93,88902

Таблица 7 – Числа активных S-блоков на соответствующих циклах при активизации одного байта входа белорусского шифра

Число активных S-блоков	Число ненулевых однобайтовых разностей в %, приходящихся на 65025 пар текстов				
	Ключ: 467e18547e73341f2a2e553b7516187233c6 67063d 402b8fad936c53c551b9e			Ключ: 270b40f162313b061e777f457caf21622 7221a4b53c24df8d3220e620d3225d	
	1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл
6	0,000000	0,000000	0,000000	0,000000	0,000000
7	0,002745	0,000000	0,000000	0,001569	0,000000
8	0,017647	0,000000	0,000000	80,030980	0,000000
9	0,190588	0,000000	0,000000	0,221569	0,000000
10	1,014510	0,000000	0,000000	1,223922	0,000000
11	0,485098	0,000000	0,000000	0,592941	0,000000
12	1,776078	0,000000	0,000000	2,171765	0,000000
13	9,105098	0,000000	0,000000	10,983529	0,000000
14	8,710196	0,000000	0,000000	10,402745	0,000000
15	3,964706	0,000000	0,000000	4,513333	0,000000
16	53,669804	0,000000	0,000000	63,663529	0,000000
17	4,491765	0,000000	0,000000	3,099216	0,000000
18	1,077647	0,000000	0,000000	0,182745	0,000000
19	15,494118	0,000000	0,000000	2,912157	0,000000
20	0,000000	0,000000	0,000000	0,000000	0,000000
21	0,000000	0,000000	0,000000	0,000000	0,000000
22	0,000000	0,000000	0,000000	0,000000	0,000000
23	0,000000	0,000000	0,000000	0,000000	0,000000
24	0,000000	0,000000	0,000392	0,000000	0,000392
25	0,000000	0,018431	0,021961	0,000000	0,020784
26	0,000000	0,472549	0,503922	0,000000	0,522745
27	0,000000	9,610980	9,993333	0,000000	10,259216
28	0,000000	90,289412	89,871765	0,000000	89,587843

свидетельствуют, что шифр Калина-2 становится случайной подстановкой после трех циклов (по дифференциальным и по линейным показателям), т.е. по динамическим показателям шифр Калина-2 имеет несколько более высокие показатели, чем шифр Rijndael (за три цикла активизируется минимум 24-ре S-блока).

Отметим далее, что, как уже отмечалось выше, в ходе разработки новой методики оценки стойкости. блочных симметричных шифров, был введен дополнительный показатель эффективности шифрующих преобразований в виде числа циклов, требующихся для прихода шифра к состоянию случайной подстановки [3]. Тот шифр считается болеесовершенным, для которого число циклов прихода к состоянию случайной подстановки оказывается меньшим.

Camellia [24]. Приведем здесь также показатели активизации S-блоков первых циклов шифра Camelia, принятого в качестве стандарта в Японии. На рис. 4 приведена конструкция *F*-функции, которая определяет преобразования на первых циклах шифра Camellia.

Camellia – это следующее поколение 128-битного блочного криптографического алгоритма, разработанного в Японии специалистами телеграфной и телефонной Корпорации Nippon и электрической Корпорации Mitsubishi, который поддерживает три размера ключей: l_k = 128, 192 и 256 бит. Блочный симметричный алгоритм Camellia был разработан не только как высоко защищенный криптографический шифр, но также как алгоритм, легко переносимый на разные аппаратные платформы. Ниже в табл. 9 приводится распределение числа активных S-блоков на

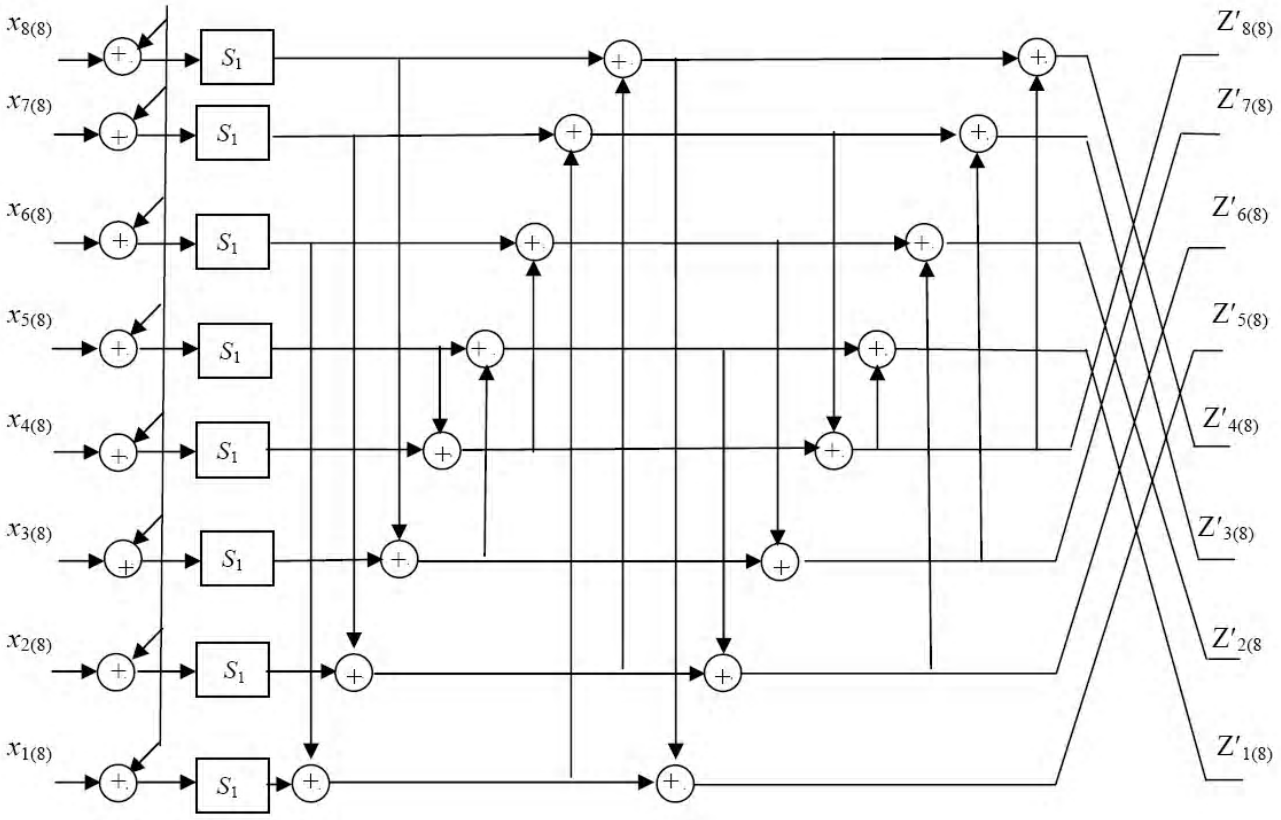

Рисунок 4 – *F*- функция\шифра Camellia

Таблица 9 – Числа активных S-блоков на соответствующих циклах при активизации одного байта входа шифра Camellia

Число активных S-блоков	Число ненулевых однобайтовых разностей в %, приходящихся на 65025 пар текстов					
	Ключ: 469c57096730bd15fd71a975c503dee469c57096730bd15fd71a975c503dee			Ключ: 46e148be3fdf41c22df55cb45ba14dcd46e148be3fdf41c22df55cb45ba14dcd		
	1-й цикл	2-й цикл	3-й цикл	1-й цикл	2-й цикл	3-й цикл
1	100	0	0	100	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	100	0,004706	0	100	0,003137
6	0	0	0,024706	0	0	0,029804
7	0	0	3,071765	0	0	3,081176
8	0	0	96,898824	0	0	96,885882

первых циклах шифрования при активизации одного байта входа шифра Camellia. Представленные результаты позволяют заключить, что шифр Camellia становится случайной подстановкой на четвертом цикле ($DP^{\pi}_{\max}= 2^{-6}$). Таким образом, по показателям случайности этот шифр уступает шифру Rijndael один цикл.

Serpent [25]. В этом 128-ми битном шифре цикловая функция строится с помощью полубайтовых S-блоков (золотых S-блоков [26]). Для таких S-блоков $DP^{\pi}_{\max}= 2^{-2}$, и, следовательно, $k_{\min}= 60$.

В табл. 10 приводится распределение активных S-блоков на первых трех циклах зашифрования для этого шифра. Из приведенных результатов следует, что шифр Serpent становится случайной подстановкой после 4-х и более циклов.

В итоге к наиболее прогрессивным из рассмотренных выше конструкций следует отнести шифры Мухомор и Калину-2, а также шифр из белорусского стандарта. Эти шифры реализуют показатели прихода к состоянию случайной подстановки близкие к предельным.

ШУП-1. В заключение мы хотим представить данные по активизации S-блоков первого цикла шифра, предложенного в патенте [27], посвященном разработке новой концепции проектирования блочных симметричных шифров. Конструкцию функции первого цикла этого шифра со 128-м битным входом иллюстрирует рис. 5.

Здесь в качестве SL преобразований применяется известная структура из 4-ех байтовых S-блоков с последующим умножением на МДР матрицу размера 4×4 (как в шифре Rijndael). На входе в первое SL преобразование выполняется сложение 32-ух битных сегментов входного блока данных по модулю 2.

Таблица 10 – Доля активных S-блоков в % на соответствующих циклах при активизации одного байта входа шифра Serpent

Число активных S-блоков	Число ненулевых повторений активизации в %, приходящихся на 65025 пар текстов		
	1-й цикл	2-й цикл	3-й цикл
1	5,490196	0	0
2	16,47058	0	0
3	27,45098	0	0
4	27,45098	0	0
5	16,47058	0	0
6	5,490196	0,1952941	0
7	0,784313	0,683921	0
8		0,1952941	0
9	0	0,6894117	0
10	0	1,0545098	0
11	0	1,0996078	0
12	0	1,1458823	0
13	0	1,2576470	0
14	0	2,9360784	0
15	0	3,5913725	0
16	0	6,3505882	0
17	0	7,0235294	0
18	0	9,0090196	0,00313725
19	0	10,6764705	0,00941176
20	0	11,1760784	0,05411764
21	0	12,0721568	0,18078431
22	0	12,2772549	0,76941176
23	0	9,17450980	2,39960784
24	0	5,70313725	7,14745098
25	0	2,79411765	16,35411764
26	0	0,79450980	27,37098039
27	0	0,09960784	29,83411764
28	0	0	15,87686274

В табл. 11 представлены результаты, иллюстрирующие активизацию S-блоков первого цикла. Видно, что с очень большой вероятностью в этой конструкции активизируются практически все 16-ть S-блоков первого цикла. Вероятность дифференциальной характеристики, составленной из 16-ти S-блоков, для $DP^{\pi}_{\max}= 2^{-6}$ (как у S-блоков шифра Rijndael) равна 2^{-96}.

5 РЕЗУЛЬТАТЫ

Полученные результаты свидетельствуют о том, что конструкции первых цикловых преобразований блочных симметричных шифров играют важную роль в обеспечении динамических показателей прихода шифров к состоянию случайной подстановки, и существенно влияют на значения числа циклов, необходимых для обеспечения запаса их стойкости. Все рассмотренные (известные) конструкции современных 128-ми битных блочных симметричных шифров, за исключением шифров IDEA NXT, Калина, Мухомор и белорусского шифра, обеспечивают динамические показатели прихода к состоянию случайной подстановки превышающие тричетыре цикла.

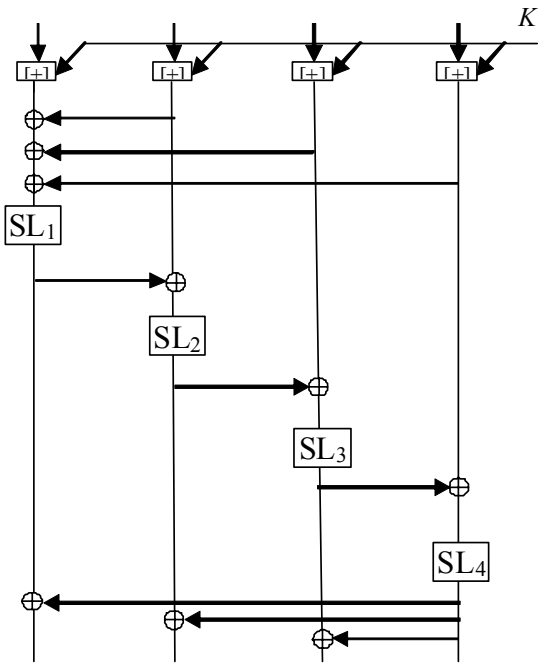

Рисунок 5 – Схема циклового преобразования шифра ШУП-1

Таблица 11 – Число активных S-блоков первого цикла

Число активных S-блоков	Доля числа активных S-блоков в %
1÷10	0
11	0,000048
12	0,000811
13	0,031328
14	0,692749
15	10,978746
16	87,905693

Шифр Rijndael оказывается далеко не в лидерах по рассматриваемому показателю (для прихода к состоянию случайной подстановки ему необходимо 4-ре цикла).

К наиболее прогрессивным решениям по построению блочных симметричных шифров можно отнести шифры ШУП-1, Калина-2, белорусский шифр и шифр Мухомор. В этих шифрах за счет активизации одним байтом входа сразу нескольких S-блоков цикловой функции обеспечивается увеличенное по сравнению с другими шифрами минимальное число S-блоков, активизируемых на первых циклах. Криптографические свойства таких шифров практически не зависят от дифференциальных и линейных свойств используемых S-блоков. А это значит, что в этих шифрах могут применяться без всяких ограничений произвольные S-блоки, порожденные генератором случайных подстановок. Для таких шифров задача поиска S-блоков с улучшенными криптографическими показателями, которой уделяется и сегодня огромное внимание в публикациях по криптографической тематике, теряет всякий смысл.

Лидером по динамическим показателям прихода шифра к состоянию случайной подстановки, безусловно, является шифр ШУП-1. Это единственный шифр, у которого на первом цикле с большой вероятностью при активизации одного байта входа активизируются все S-блоки цикловой функции. В этом шифре благодаря отмеченным высоким динамическим показателям применяется восемь циклов зашифрования (существенно меньше, чем у шифров Rijndael и Калина). Более того в этом шифре допускается конвейерная обработка данных, позволяющая дополнительно повысить скорость шифрования почти в три раза. Наконец в этом шифре применена существенно более быстродействующая по сравнению с шифром Калина схема разворачивания ключей.

6 ОБСУЖДЕНИЕ

Предложенные в работах [3, 4, 5] вычислительный, и дополненный в этой работе экспериментальный методы определения динамических показателей прихода блочных симметричных шифров к состоянию случайной подстановки позволяют для полномасштабных версий проверяемых шифров оценить минимальное число циклов шифрования, после которых шифры приходят к состоянию случайной подстановки. В итоге открываются дополнительная возможность для сравнения по эффективности шифров между собой.

В то же время знание показателей прихода шифров к состоянию случайной подстановки позволяет обосновано подойти к определению числа циклов зашифрования, обеспечивающих необходимый запас стойкости шифров. Как показала практика, этот запас выбирается в три-четыре раза превышающим число циклов шифрования, необходимое для прихода шифра к состоянию случайной подстановки. Например, для 512 битного шифра Калина-2 выбранное число циклов зашифрования 18 является явно завышенным. Как показывают наши оценки, 512 битный шифр Калина-2 приходит к состоянию случайной подстановки за четыре цикла. А это означает, что для него без снижения стойкости можно ограничиться 12-ю циклами зашифрования, что позволяет повысить быстродействие шифра более чем в 1,5 раза.

Перспективы дальнейших исследований видятся в разработке дополнительных усовершенствований уже существующих конструкций шифров в направлении улучшения их динамических показателей прихода к случайной подстановке, что позволит применять в усовершенствованных шифрах S-блоки случайного типа. Первое предложение в этом направлении уже запатентовано [28].

ВЫВОДЫ

В работе решена задача уточнения и подтверждения с помощью вычислительных экспериментов эффективности новой методики оценки динамических показателей прихода итеративных блочных симметричных шифров к состоянию случайной подстановки.

Научная новизна результатов статьи состоит в том, что впервые получены обоснованные объективные данные для значений числа циклов прихода к состоянию случайной подстановки ряда современных шифров.

Практическая значимость предлагаемой методики и представленных в работе результатов видится в их конструктивизме. Они позволяют выполнить обоснование числа циклов шифрующих преобразований, которые обеспечивают достижение предельного уровня стойкости шифров.

БЛАГОДАРНОСТИ

Работа выполнена в рамках госбюджетной научно-исследовательской темы Харьковского национального университета им. В. Н. Каразина «Аналіз стану, обґрунтування вимог та напрямків розвитку, стандартизація розробка та впровадження криптографічних систем для надання електронних довірчих послуг» (номер гос. регистрации 0116U000810). Приказ МОН Украины № 158 от 26.02.2016 г.

СПИСОК ЛИТЕРАТУРЫ

1. Лисицкая И. В. Методология оценки стойкости блочных симметричных криптопреобразований на основе уменьшенных моделей: дис. … докт. техн. наук: 05.13.05 / Лисицкая Ирина Викторовна. – Харьков, 2012. – 293 с.
2. Долгов В. Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа : монография / В. И. Долгов, И. В. Лисицкая. – Харьков : Издательство «Форт», 2013. – 420 с.
3. Горбенко И. Д. О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями нелинейности близкими к предельным / И. Д. Горбенко, К. Е. Лисицкий // Радиотехника : Всеукр. межвед. Науч.-техн. сб. – 2014. – Вып. № 176. – С. 27–39.
4. Gorbenko I. D. On Ciphers Coming to a Stationary State of Random Substitution / I. D. Gorbenko, K. E. Lisitskiy, D. S. Denisov // Universal Journal of Electrical and Electronic Engineering, – No. 2. – P. 206–215. DOI. 10.13189/ujeee. 2014.020409.
5. Лисицкий К. Е. Динамические показатели прихода блочных шифров к состоянию случайной подстановки / К. Е. Лисицкий // Издательский дом LAP LAMBERT Academic Publishing, 2014. – 60 с. ISBN-13. 978-3-659-28919-4.
6. Keliher L. Improving the upper bound on the maximum average linear hull probability for Rijndael / L. Keliher, H. Meijer and S. Tavares // Advances in Cryptology, Selected Areas in Cryptography ’01, LNCS 2259, S. Vaudenay, A. M. Youssef, Eds., Springer-Verlag. – 2001. – P. 112–128.
7. On the security of Rijndael-like structures against differential and linear cryptanalysis / [S. Park, S. H. Sung, S. Chee et al.] // Advances

in Cryptology, Proceedings of Asiacrypt '02, LNCS 2501, Y. Zheng, Ed., Springer-Verlag. – 2002. – P. 176–191.
8. Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES / [S. Park, S. H. Sung, S. Lee et al.] // Fast Software Encryption '03, LNCS 2887, T. Johansson, Ed., Springer-Verlag. – 2003. – P. 247–260.
9. Vaudenay S. Resistance against general iterated attacks / S. Vaudenay // Advances in Cryptology, Proceedings of Eurocrypt '99, LNCS 1592, J. Stern, Ed., Springer-Verlag. – 1999. – P. 255–271.
10. Matsui M. On a Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis / M. Matsui // IEICE Trans/ FundaMENTALS. – January 1999. – Vol. E82-A, No. 1. – P. 117–122.
11. Provable Security against Differential and Linear cryptanalysis for SPN Structure / [S. Hong, S. Lee, J. Lim et al.] // B. Schneier (Ed.): FSE 2000, LNCS. – 1978. – P. 273–283, 2001.
12. Baignoires T. Proving the Security of AES Substitution-Permutation Network / T. Baignoires, S. Vaudenay // http://lasecwww.epfl.ch. – 2004. – P. 16.
13. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и относительно алгебраических атак, основанных на гомоморфизмах. / [Алексийчук А. Н., Ковальчук Л. В., Скрыпник Е. В. и др.] // Прикладная радиоэлектроника. – 2008. – Т. 7, № 3. – С. 203–209.
14. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis / [F. Sano, K. Ohkuma, H. Shimizu et al.] // IEICE Trans. Fundamentals. – January 2003. – Vol. E86-a, No.1. – P. 37–46.
15. Лисицкая И. В. О криптографической значимости схем разворачивания ключей в обеспечении стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / И. В. Лисицкая, А. А. Настенко, К. Е. Лисицкий // Радиоэлектроника и информатика. – 2012 – № 3 (58). – С. 56–65.
16. Дифференциальные свойства подстановок / [Р. В. Олейников, О. И. Олешко, К. Е. Лисицкий и др.] // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 326–333.
17. Долгов В. И. Свойства таблиц линейных аппроксимаций случайных подстановок / В. И. Долгов, И. В. Лисицкая, О. И. Олешко // Прикладная радиоэлектроника. – 2010. – № 3. – С. 334–340
18. 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. – № 960, Вип.16. – С. 196–206.
19. Daemen J. AES Proposal: Rijndael / J. Daemen and V. Rijmen. 1st AES Conference, California, USA. – 1998. – [Электронный ресурс] Режим доступа: http://www.nist.gov/aes.
20. Junod P. FOX: a new family of block ciphers / P. Junod and S. Vaudenay // In H. Handschuh and A. Hasan, editors, Selected Areas in Cryptography: 11th International Workshop, SAC 2004, Waterloo, Canada, August 9–10, 2004. Revised Selected Papers, volume 3357 of Lecture Notes in Computer Science, Springer-Verlag. – 2004. – P 114–129.
21. Перспективный блочный симметричный шифр «Мухомор» – основные положения и спецификация / [Горбенко И. Д., Бондаренко М. Ф., Долгов В. И. и др.] // Прикладная радиоэлектроника. – 2007. – Том. 6, № 2. – С. 147–157.
22. Государственный стандарт республики Беларусь. СТБ 34.101.31-2011. Информационные технологии. Защита информации Криптографические алгоритмы шифрования и контроля целостности. Введен в действие постановлением Госстандарта Республики Беларусь от 31 января 2011 г. № 5. Изд-во Госстандарт, Минск. – 2011. – 35 с.
23. Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К. : Держспоживстандарт України, 2015. – 238 с. – (Національний стандарт України).
24. Specification of Camellia – a 128 bit Block Cipher, version 2.0 / [K. Aoki, T. Ichikawa, M. Kanda et al.] // Copyringht NTT and Mitsubishi Tlektronic Corporation. – 2001. – September 26. – P. 35.
25. Biham E. Serpent: A New Block Cipher Proposal / E. Biham, R. Anderson, and L. R. Knudsen // In S. Vaudenay, editor, 5th Fast Software Encryption Workshop, LNCS 1372. – Springer-Verlag. – 1998. – P. 222–238.
26. Markku J. Cryptographic Analysis of All 16-Bit S-Boxes / Markku-Juhani, O. Saarinen // – 2008. – Vol. 7118 of the series Lecture Notes in Computer Science. – P. 118–133.
27. Пат. 111547 Україна, МПК (2016.01) G09C 1/00 H04L 9/06 (2006.01). Спосіб криптографічного перетворення двійкових даних (варіанти) / Горбенко І. Д., Долгов В. І., Лисицька І. В. та інші (Україна); заявник АО ІІТ м. Харків. № a201500942; заявл. 06.02.2015; опубл. 10.05.2016, Бюл. № 9. – 20 с.
28. Пат. 111448 Україна, МПК H04L 29/14 (2006.01) H04L 9/14 (2006.01) H04L 9/06 (2006.01). Спосіб криптографічного перетворення двійкових даних / Горбенко І. Д., Долгов В. І., Лисицька І. В. та інші (Україна); заявник АО ІІТ м. Харків. № a201503976; заявл. 25.04.2015; опубл. 25.04.2016, Бюл. № 8 – 20 с.

Статья поступила в редакцию 29.08.2016.
После доработки 03.10.2016.

Лисицька І. В.[1], Лисицький К.Є.[2], Головко І. А.[3], Жаріков І. І.[3], Корнієнко М. А.[3], Кулеба М. В.[3], Родінко М. Ю.[3]

[1]Д-р техн. наук, професор, професор кафедри Безпеки Інформаційних Систем і Технологій Харківського національного університету ім. В. Н. Каразіна, Харків. Україна

[2]Студент Харківського національного університету ім. В. Н. Каразіна, Харків. Україна

[3]Студенти Харківського національного університету радіоелектроніки, Харків, Україна

ЕКСПЕРИМЕНТАЛЬНІ ДАНІ ЩОДО ВИЗНАЧЕННЯ ДИНАМІЧНИХ ПОКАЗНИКІВ ПРИХОДУ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ ДО СТАНУ ВИПАДКОВОЇ ПІДСТАНОВКИ

Актуальність. Об'єктом досліджень даної роботи є процеси приходу блокових симетричних шифрів до стану випадкової підстановки.

Мета роботи. Уточнення за допомогою обчислювальних експериментів значень динамічних показників приходу ряду сучасних шифрів до стану випадкової підстановки, які можуть стати важливими при порівняльній оцінці їх ефективності.

Метод. Методика виконання експериментів при визначенні диференціальних показників полягає в активізації шифрів (програмних моделей) наборами вхідних різниць і подальшого визначення мінімальної кількості S-блоків, що активізується на перших циклах шифрування, що дозволяє отримати значення диференціальної ймовірності відповідне показнику стійкості розглянутого шифру. При визначенні лінійних показників перебираються ненульові маски входів в S-блоки і ненульові маски їх виходів. При цьому на вході шифру активізується один байт вхідного блоку даних, причому вибирається байт, який активізує мінімальне число S-блоків першого циклу. Тут під активним байтом (S-блоком) розуміється байт (S-блок), за допомогою якого для пари входів в шифр (в S-блок) формується ненульова вхідна (вихідна) різниця. Потім в режимі шифрування повним перебором всіх 256 бітових однобайтових різниць входу

шифру визначається мінімальне число S-блоків, що активізується на кожному з циклів, які перераховуються в числа циклів шифрування, необхідних для приходу шифру до випадкової підстановки. Близька за змістом процедура може бути виконана і при аналізі лінійних показників з використанням вхідних і вихідних масок.

Результати. Отримані результати свідчать про те, що конструкції перших циклових перетворень блокових симетричних шифрів грають важливу роль в забезпеченні динамічних показників приходу шифрів до стану випадкової підстановки, і істотно впливають на значення числа циклів, необхідних для забезпечення запасу їх стійкості. Всі розглянуті (відомі) конструкції сучасних 128-ми бітних блокових симетричних шифрів, за винятком шифрів IDEA NXT, Калина, Мухомор і білоруського шифру, забезпечують динамічні показники приходу до стану випадкової підстановки, що перевищують три-чотири цикли. Шифр Rijndael виявляється далеко не в лідерах з даного показника (для приходу до стану випадкової підстановки йому необхідно 4-ри цикли).

Висновки. В роботі вирішена задача уточнення і підтвердження за допомогою обчислювальних експериментів ефективності нової методики оцінки динамічних показників приходу шифрів до стану випадкової підстановки.

Наукова новизна результатів статті полягає в тому, що вперше отримані обгрунтовані об'єктивні дані для значень числа циклів приходу до стану випадкової підстановки ряду сучасних шифрів.

Практична значимість запропонованої методики і представлених в роботі результатів полягає в їх конструктивізм. Вони дозволяють виконати обгрунтування числа циклів шифруючих перетворень, які забезпечують досягнення граничного рівня стійкості шифрів.

Ключові слова: блоковий симетричний шифр, динамічні показники, стан випадкової підстановки, стійкість до атак диференціального і лінійного криптоаналізу, активні S-блоки.

Lisitskaya I. V.[1], Lisitsky K. E.[2], Golovko I. A.[3], Zharikov I. I.[3], Kornienko M. A.[3], Kuleba M. V.[3], Rodinko M. Y.[3]

[1]Dr. Sc., Professor, Professor of department of Security of Information Systems and Technologies of the V. N. Karazin Kharkov National University, Kharkov, Ukraine

[2]Student of the V. N. Karazin Kharkov National University, Kharkiv, Ukraine

[3]Students of the Kharkov National University of Radio Electronics, Kharkov, Ukraine

EXPERIMENTAL DATA FOR THE IDENTIFICATION OF DYNAMIC INDICATORS OF COMING TO BLOCK OF SYMMETRIC CIPHERS RANDOM PERMUTATION

Context. The object of study of this work is the arrival processes of block symmetric ciphers to the state of a random permutation.

Objective. Clarification by means of computational experiments values of dynamic parameters arrival of some modern ciphers to the state of a random permutation, which can be important when evaluating their effectiveness.

Method. Methods of experiments consists in determining the differential parameters in activation ciphers (programming models) sets the input difference and the subsequent determination of the minimum number of S-boxes-activated in the first cycle of encryption, allowing to obtain the value of the differential probability of relevant indicators of resistance considered cipher. In determining the linear indicators are moving non-zero mask inputs in S-boxes, and non-zero mask their outputs.

When this input is activated on one cipher byte input frame, with a byte is selected, which activates minimum number the first cycle of S-blocks. Here, the active byte (S-unit) means bytes (S-unit), by which for the pair in the input code (in the S-box) is formed non-zero input (output) the difference. Then, in the mode of encoding a complete listing of all 256 bit single-byte cipher input differences determined by the minimum number of activatable S-boxes in each of the cycles that are translated into the number of encsphering cycles required for the arrival of a random permutation cipher. A similar within the meaning of the procedure can be performed in the analysis of linear parameters using the input and output masks.

Results. The results indicate that the construction of the first cyclic transformation block symmetric ciphers play an important role in ensuring the dynamic performance of the parish codes to random permutation, and significantly affect the value of the number of cycles required for the stock of their resistance. All of the (known) design of modern 128-bit block symmetric ciphers, except ciphers IDEA NXT, Kalina, Amanita and Belarusian cipher, provide dynamic performance to the arrival of a random permutation exceeding three or four cycles. Rijndael cipher is far from the leaders of the subject indicator (for the arrival of a random permutation it needs 4 cycles).

Conclusions. In this paper we solve the problem clarification and confirmation via computational experiments the effectiveness of a new methodology for assessing the dynamic performance of the parish codes to random permutation.

Scientific novelty of the results of the paper is that the first objective data obtained reasonable for the arrival of number of cycles to the values of a random permutation of some modern ciphers.

The practical significance of the proposed methodology and presented the results is their constructivism. They allow you to perform a study of ciphering transformation cycles that achieve the maximum level of resistance ciphers.

Keywords: block symmetric cipher, dynamic indicators, state random permutation, resistance to differential and linear attacks cryptanalysis, the active S-boxes.

REFERENCES

1. Lisitskaya I. V. Metodologiya ocenki stojkosti blochnyh simmetrichnyh kriptopreobrazovanij na osnove umenshenyh modelej diss. Doctor. Tehn. Sciences: 05.13.05. Kharkov, 2012, 293 p.
2. Dolgov V. I., Lisitskaya I. V. Metodologiya ocenki stojkosti blochnyh simmetrichnyh shifrov k atakam differencial'nogo i linejnogo kriptoanaliza: monografiya. Har'kov. Izdatel'stvo «Fort», 2013, 420 p.
3. Gorbenko I. D., Lisitskij K. E. O dinamike prihoda shifrov k sluchajnoj podstanovke pri ispol'zovanii S-blokov s pokazatelyami nelinejnosti blizkimi k predel'nym, *Radiotehnika: Vseukr. Mezhved. Naych.- tehn. zb*., 2014, Vyp. № 176, pp. 27–39.
4. Gorbenko I. D. Lisitskiy K. E., Denisov D. S. On Ciphers Coming to a Stationary State of Random Substitution, *Universal Journal of Electrical and Electronic Engineering*, No. 2 , pp. 206– 215. DOI: 10.13189/ujeee. 2014.020409.
5. Lisitskij K. E. Dinamicheskie pokazateli prihoda blochnyh shifrov k sostoyaniyu sluchajnoj podstanovki, *Izdatel'skij dom LAP LAMBERT Academic Publishing,* 2014, 60 p. ISBN-13: 978-3-659-28919-4.
6. Keliher L., Meijer H., and Tavares S. Improving the upper bound on the maximum average linear hull probability for Rijndael, *Advances in Cryptology, Selected Areas in Cryptography '01, LNCS 2259, S. Vaudenay, A. M. Youssef,* Eds. Springer-Verlag, 2001, pp. 112–128.
7. Park S., Sung S. H., Chee S. et al. On the security of Rijndael-like structures against differential and linear cryptanalysis, *Advances in Cryptology, Proceedings of Asiacrypt '02, LNCS 2501, Y. Zheng*, Ed., Springer-Verlag, 2002, pp. 176–191.

8. Park S., Sung S.H., Lee S. et al. Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES, *Fast Software Encryption '03, LNCS 2887, T. Johansson*, Ed. Springer-Verlag, 2003, pp. 247–260.
9. Vaudenay S. Resistance Against General Iterated Attacks, *Advances in Cryptology, Proceedings of Eurocrypt '99, LNCS 1592, J. Stern,* Ed., Springer-Verlag, 1999, pp. 255–271.
10. Matsui M. On a Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis. IEICE Trans/ FundaMENTALS, Vol. E82-A, No. 1 January 1999, pp. 117–122.
11. Hong S., Lee S., Lim J. et al. Provable Security against Differential and Linear cryptanalysis for SPN Structure, *B. Schneier (Ed.): FSE 2000, LNCS,* 1978, 2001, pp. 273–283.
12. Thomas B., Vaudenay S. Proving the Security of AES Substitution-Permutation Network. http://lasecwww.epfl.ch., 2004, p. 16.
13. Aleksijchuk A. N., Kovalchuk L. V., Skrupnik E. V. i dr. Ocenki prakticheskoj stojkosti blochnogo shifra «Kalina» otnositelno metodov raznostnogo, linejnogo kriptoanaliza otnositelno algebraicheskih atak, osnovannyh na gomomorfizmah, *Prikladnaya Radioelektronika,* 2008, Vol. 7, No. 3, pp. 203–209.
14. Sano F., Ohkuma K., Shimizu H. et al. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis, *IEICE Trans. Fundamentals*, Vol. E86-a, No. 1, January 2003, pp. 37–46.
15. Lisitskaya I. V. Nastenko A. A., Lisitskij K. E. O kriptograficheskoj znachimosti shem razvorachivaniya klyuchej v obespechenii stojkosti blochnyh simmetrichnyh shifrov k atakam differencial'nogo i linejnogo kriptoanaliza, *Radioelektronika i informatika,* 2012, No. 3(58), pp. 56–65.
16. Olejnikov R. V., Oleshko O. I., Lisitskij K. E. i dr. Differencial'nye svojstva podstanovok, *Prikladnaya Radioelektronika*, 2010, Vol. 9, No. 3, pp. 326–333.
17. Dolgov V. I., Lisitskaya I. V., Oleshko O. I. Svojstva tablic linejnyh aproksimacij sluchajnuh podstanovok, *Prikladnaya Radioelektronika,* 2010, No. 3, pp. 334–340
18. Lisitskaya I.V. Svojstva zakonov raspredeleniya XOR tablic i tablic linejnyh aproksimacij sluchajnyh podstanovok, *Visnyk Harkovskogo nacional'nogo universiteta im. V.N. Karazina,* 2011, No. 960, Vup.16, pp. 196–206.
19. Daemen J., Rijmen V. AES Proposal: Rijndael, *1st AES Conference*. California, USA, 1998. [Electronic resourse] Access mode: http:/ /www.nist.gov/aes.IDEA NXT
20. Junod P., Vaudenay S. FOX: a new family of block ciphers, *In H. Handschuh and A. Hasan, editors, Selected Areas in Cryptography*: *11th International Workshop, SAC 2004.* Waterloo, Canada, August 9–10, 2004, Revised Selected Papers, volume 3357 of Lecture Notes in Computer Science, Springer-Verlag, 2004, pp. 114–129
21. Gorbenko I. D., Bondarenko M. F., Dolgov V. I. i dr. Perspektivnyj blochnyj simmetrichnyj shifr «Muhomor» – osnovnye polozheniya i specifikaciya, *Prikladnaya Radioelektronika,* 2007. Vol. 6, No. 2, pp. 147–157.
22. Gosudarstvennyj standart respubliki Belarus'. STB 34.101.31-2011. Informacionnye tehnologii. Zashita informacii. Kriptograficheskie algoritmy shifrovaniya i kontrolya celostnosti. Vveden v dejstvie postanoveniem Gosstandarta Respubliki Belarus' ot 31 yanvarya 2011 g. № 5. Izd-vo Gosstandart. Minsk, 2011, 35 p.
23. Informacijni tehnologii. Kriptografichnyj zahyst informacii. Algoritm symmetrichnogo blokovogo peretvorennya: DSTU 7624:2014. Kiev, Derzhspozhyvstandart Ukrainu, 2015, 238 p. (Nacional'nyj standartUkrainy).
24. Aoki K., Ichikawa T., Kanda M. et al. Specification of Camellia – a 128 bit Block Cipher, version 2.0, *Copyringht NTT and Mitsubishi Tlektronic Corporation*, 2001, September 26, pp. 35.
25. Biham E., Anderson R., and Knudsen L. R. Serpent: A New Block Cipher Proposal. In S. Vaudenay, editor, 5th Fast Software Encryption Workshop, LNCS 1372, Springer-Verlag, 1998, pp. 222–238.
26. Markku-Juhani O. Saarinen Cryptographic Analysis of All 16-Bit S-Boxes. 2008. Volume 7118 of the series Lecture Notes in Computer Science, pp. 118–133.
27. Gorbenko I. D., Dolgov V. I., Lisitskaya et al. (Ukraina) Pat 111547 Ukraina, МПК (2016.01) G09C 1/00 H04L 9/06 (2006.01). Sposib kryptografichnogo peretvorennya dvijkovyh danyh (varianty) / ; zayavnyk AO IIT m. Charkiv. № a201500942; zayavleno 06.02.2015; opublikovano 10.05.2016, Bull. № 9, 20 p.
28. Gorbenko I. D., Dolgov V. I., Lisitskaya et al. (Ukraina)Pat. 111448 Ukraina, МПК H04L 29/14 (2006.01) H04L 9/14 (2006.01) H04L 9/06 (2006.01). Sposib kryptografichnogo peretvorennya dvijkovyh danyh ; zayavnyk AO IIT m. Charkiv. № a201503976; zayavleno 25.04.2015; opublikovano 25.04.2016, Bull. № 8, 20 p.