УДК 621. 3.06

В.И. ДОЛГОВ, д-р техн. наук, И.В. ЛИСИЦКАЯ, д-р техн. наук, К.Е. ЛИСИЦКИЙ

УСОВЕРШЕНСТВОВАННЫЙ БЛОЧНЫЙ СИММЕТРИЧНЫЙ ШИФР КАЛИНА

Введение

В соответствии с новой (усовершенствованной) концепцией построения блочных симметричных шифров (БСШ) [1] предлагается первый цикл шифрующего преобразования строить так, чтобы активизировалось как можно больше S-блоков (в предельном случае все S-блоки) первого цикла шифрующего преобразования. Для реализации этого подхода было предложено использовать три метода:

1. Применение наряду с принятым в известных разработках параллельным запуском S-блоков цикловой функции входными блоками данных операции последовательного их запуска одного за другим;

2. Использование в первом цикле увеличенного числа S-блоков, обеспечивающего при активизации всего их множества предельные для шифра значения максимальных дифференциальных и линейных вероятностей;

3. Введение дополнительного смешивающего преобразования на входе шифра.

Эти предложения подкреплены разработками. В шифре ШУП-1 [2] применены первый и третий методы, в шифре ШУП-2 [1] применены все три отмеченные методы, а в усовершенствованном шифре Rijndael [3] реализован третий метод. Результатами этих предложений стало обеспечение улучшенных динамических показателей прихода новых шифров к состоянию случайной подстановки. Все они становятся случайными постановками за один-два цикла. Кроме возможности уменьшения числа циклов зашифрования при рассматриваемом подходе удается снять ограничения на дифференциальные и линейные показатели S-блоков, используемых при построении цикловых преобразований, что оказывается немаловажным для отбора подходящих S-блоков.

В последнее время возродился интерес к дальнейшему наращиванию показателей стойкости блочных симметричных шифров в направлении расширения мощности ключевого множества. Такая возможность видится в том, чтобы сделать ключезависимыми (сменными) и узлы замены (блоки подстановок), как в свое время это было сделано в шифре ГОСТ 28147-89. И тогда возникает задача оценки степени дополнительного расширения мощности ключевого множества за счет применения сменных узлов замены.

Заметим, что известные подходы к выбору узлов замены опираются на поиск S-блоков с улучшенными в первую очередь дифференциальными и линейными показателями, так как считается, что эти показатели существенно влияют на показатели стойкости всего шифра. Эти подходы реализованы в шифрах Rijndael, Camellia, Мухомор, ADE, Калина и ряде других, в том числе и последних разработок.

В то же время, как следует из новой методологии оценки стойкости блочных симметричных шифров [4], результирующие показатели стойкости шифров не зависят от используемых в них S-блоков. Подстановочные преобразования (S-блоки) влияют лишь на динамику прихода шифров к состоянию случайной подстановки. Наши подходы к проектированию БСШ направлены на улучшение динамических показателей прихода шифров к состоянию случайной подстановки, что позволяет практически снять ограничения на отбор S-блоков, пригодных для использования в шифре. Имеется в виду, что по нашим результатам в качестве S-блоков в таких шифрах могут быть практически использованы S-блоки, сгенерированные случайным образом без всяких ограничений. Такой подход, как мы убедимся в дальнейшем, позволяет существенно расширить мощность множества подстановок, пригодных для использования в качестве сменных узлов замены.

В этой работе мы хотим воспользоваться развиваемым подходом для улучшения показателей случайности шифра Калина и, в частности, нового украинского стандарта [5]. Будет показано, что усовершенствованная версия шифра Калина допускает использование случайно порожденных S-блоков. Приведем также оценки для множества случайных подстановок при использовании их в наших шифрах в качестве сменных узлов замены.

1.Суть предложений

Приведем решения для всех трех вариантов блочного размера шифра Калина.

Напомним структуру циклового преобразования шифра Калина [6]. В шифре Калина сохранены все базовые операции шифра Rijndael. Его отличие от шифра Rijndael состоит в использовании разных S-блоков (восемь разных S-блоков, отобранных специальным образом), вместо одинаковых S-блоков, построенных по конструкции, предложенной К. Нюберг, и применении попеременного сложения с цикловыми подключами по модулю 2 и по модулю 2^{32} (последней операции нет в Rijndael-е, там все цикловые ключи вводятся с помощью операции сложения по модулю 2). Кроме того, линейное преобразование выполняется с помощью матрицы МДР кода размера 8×8 над полем GF(2^8) (в шифре Rijndael линейное преобразование выполняется тоже с помощью матрицы МДР кода над полем GF(2^8), но размера 4×4). Кроме того, в шифре Калина в последнем цикле исключена операция ShiftRows. Наконец, в шифре использована оригинальная схема разворачивания ключей.

Напомним здесь также операцию перестановки элементов, так как она будет влиять на вводимую операцию дополнительного преобразования. В спецификации шифра эта функция обозначена как τ_l. Операция τ_l выполняет циклический сдвиг влево строк матрицы состояний. Число элементов сдвига зависит от номера строки $i \in \{0,1,..,7\}$, размера блока $l \in \{128,256,512\}$ и вычисляется по формуле $\delta_i = \left\lfloor \frac{i \cdot l}{512} \right\rfloor$. Это значит, что для 128-битного шифра первые четыре строки матрицы состояний, состоящей из двух 64-битных колонок, остаются без изменения, а в последующих четырех строках элементы меняются местами. Для 256-битного шифра матрица состояний состоит уже из четырех колонок, и функция τ_l осуществляет последовательный сдвиг двух строк матрицы на один байт. Для 256-битного шифра матрица состояний состоит из восьми колонок, и функция τ_l осуществляет последовательный сдвиг каждой строки на один байт.

В основе дальнейшего материала лежит разработка по построению усовершенствованного шифра Rijndael [3], защищенная патентом [7].

Первое предложение ориентировано на 128-битную версию шифра.

Здесь введенная дополнительная операция повторяет операцию, использованную в предложении [3].

Схема усовершенствованного шифра Калина представлена на рис. 1.

Обозначение $\oplus$ соответствует побитному суммированию по модулю два (XOR).

Дополнительная инволютивная операция вводится на входе шифра после операции забеливания. 32-битные сегменты входного блока данных (X_1,X_2,X_3,X_4), как и в [3], подвергаются операции смешивания между собой по три, так что вместо четвертого сегмента формируется сумма по модулю два второго, четвертого и третьего сегментов ($X_2 \oplus X_3 \oplus X_4$), вместо третьего сегмента формируется сумма по модулю два первого, третьего и второго сегментов ($X_1 \oplus X_2 \oplus X_3$), вместо второго сегмента формируется сумма по модулю два второго, третьего и четвертого сегментов ($X_1 \oplus X_2 \oplus X_4$), вместо первого сегмента формируется сумма по модулю два первого, третьего и четвертого сегментов ($X_1 \oplus X_3 \oplus X_4$), далее после конкатенации полученных результатов выполняются уже оригинальные операции шифра Калина-128.

Это позволяет реализовать первоначальное доцикловое преобразование, обладающее улучшенными перемешивающими и рассеивающими свойствами, в частности добиться полного исключения детерминированного получения характеристик с одним активным байтом на входе первого цикла.

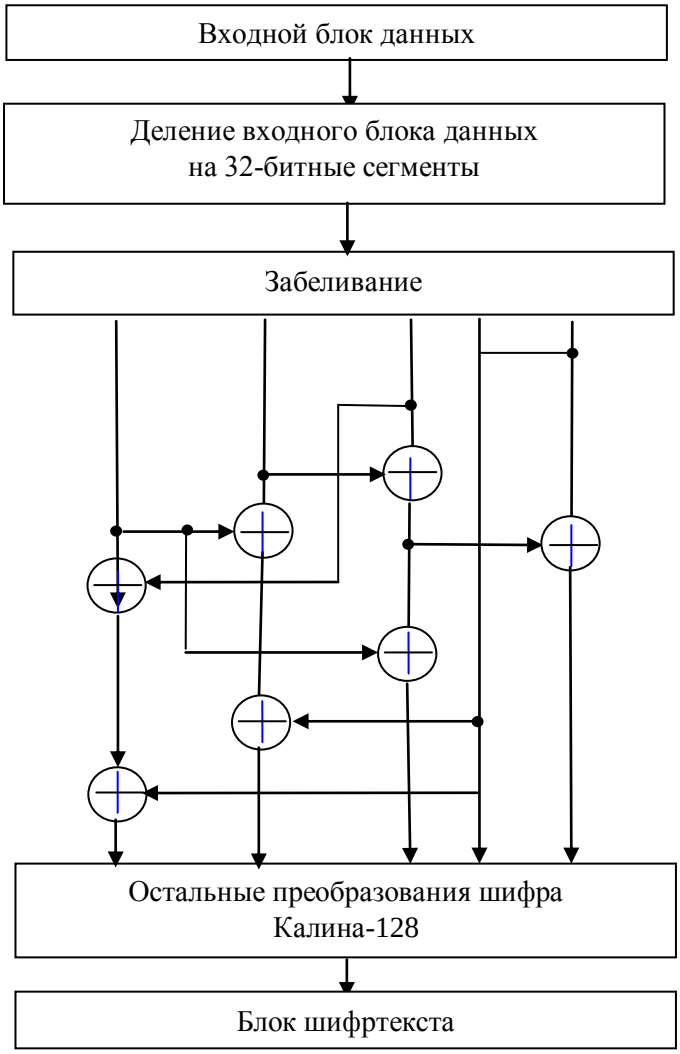

Рис. 1

Как следует из представленных данных, каждый байт входного блока данных присутствует в обеих колонках. Это значит, что один активный байт на входе усовершенствованной Калины-128 будет активизировать минимум три S-блока первого цикла (один S-блок в одной колонке матрицы состояний и два S-блока – во второй).

Рис. 2 иллюстрирует распределение байтов в матрице состояний первого цикла после операции сдвига строк.

$$
\begin{array}{cc}
b_1 \oplus b_9 \oplus b_{13} & b_1 \oplus b_5 \oplus b_9 \\
b_2 \oplus b_{14} \oplus b_{10}, & b_2 \oplus b_6 \oplus b_{10} \\
b_3 \oplus b_{11} \oplus b_{15} & b_3 \oplus b_7 \oplus b_{11} \\
b_4 \oplus b_{12} \oplus b_{16} & b_4 \oplus b_8 \oplus b_{12} \\
b_1 \oplus b_5 \oplus b_{13} & b_5 \oplus b_9 \oplus b_{13} \\
b_2 \oplus b_6 \oplus b_{14} & b_6 \oplus b_{10} \oplus b_{14} \\
b_3 \oplus b_7 \oplus b_{15} & b_7 \oplus b_{11} \oplus b_{15} \\
b_4 \oplus b_8 \oplus b_{16} & b_8 \oplus b_{12} \oplus b_{16}
\end{array}
\longrightarrow
\begin{array}{cc}
b_1 \oplus b_9 \oplus b_{13} & b_1 \oplus b_5 \oplus b_9 \\
b_2 \oplus b_{10} \oplus b_{14} & b_2 \oplus b_6 \oplus b_{10} \\
b_3 \oplus b_{11} \oplus b_{15} & b_3 \oplus b_7 \oplus b_{11} \\
b_4 \oplus b_{12} \oplus b_{16} & b_4 \oplus b_8 \oplus b_{12} \\
b_5 \oplus b_9 \oplus b_{13} & b_1 \oplus b_5 \oplus b_{13} \\
b_6 \oplus b_{10} \oplus b_{14} & b_2 \oplus b_6 \oplus b_{14} \\
b_7 \oplus b_{11} \oplus b_{15} & b_3 \oplus b_7 \oplus b_{15} \\
b_8 \oplus b_{12} \oplus b_{16} & b_4 \oplus b_8 \oplus b_{16}
\end{array}
$$

Рис. 2

Видно, что на втором цикле с очень большой вероятностью будут активизироваться все 16 S-блоков, а на трех циклах следует ожидать активизации при одном активном байте входа 35 S-блоков.

В табл. 1 – 3 приводятся результаты экспериментов по оценке числа активных S-блоков первых циклов при активизации одного и двух байтов входа усовершенствованного 128-битного шифра.

Таблица 1

Число активных S-блоков	Число ненулевых однобайтовых разностей, %	
	1-й цикл	2-й цикл
1	0	0
2	0	0
3	44,133	0
4	49,7549	0
5	6,11213	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0,0428922
15	0	3,35172
16	0	96,6054

Таблица 2

Число активных S-блоков	Число ненулевых однобайтовых разностей, %	
	1-й цикл	2-й цикл
1	0	0
2	0	0
3	0,362759	0
4	0,382193	0
5	0,22049	0
6	42,5443	0
7	49,2525	0
8	7,09436	0
9	0,141907	0
10	0	0
11	0	0,00000014
12	0	0,00002739
13	0	0,00286027
14	0	0,1744
15	0	5,871177
16	0	93,95

Таблица 3

Число активных S-блоков	Число ненулевых однобайтовых разностей, %	
	1-й цикл	2-й цикл
1	0	0
2	0	0
3	0,000000536	0
4	0,000011967	0
5	0,000208	0
6	0,0035186	0
7	0.0723077	0
8	0,441418	0
9	0,660915	0
10	7,99482	0
11	53,2098	0,0000003.9736
12	36,8236	0,0000410688
13	0,793344	0,003.16625
14	0	0,173342
15	0	5,89352
16	0	93,9299

В первом случае (табл. 1) на вход шифра подавались однобайтовые разности (активизировался самый правый байт входа.), во втором (табл. 2) активизировались одинаковыми разностями 12-й и 16-й байты, а остальные байты брались нулевыми, а в третьем (рис. 3) активизировались одинаковыми разностями 6-й и 10-й байты входа, а остальные байты брались нулевыми.

Модульное сложение (с переносом разрядов) на входе шифра, как следует из данных табл. 1 и 2, обеспечивает активизацию обеих колонок матрицы состояний (при активизации колонок матрицы состояний даже в том случае, когда активизируются байты входа двумя соседними байтами).

В табл. 4 представлены результаты вычислительного эксперимента в процентах по определению числа активных S-блоков для трех первых циклов шифра Калина-128. Рассматривались ненулевые разности для самого левого и самого правого байтов входа. Результаты, полученные для самого левого и самого правого байта входного блока данных, получились идентичными. Представленные результаты свидетельствуют, что шифр Калина становится случайной подстановкой по дифференциальным показателям после трех циклов зашифрования. Минимальное число активизируемых S-блоков для шифра с “родными” подстановками получается равным 25.

Таблица 4

Число активных S-блоков	Число ненулевых однобайтовых разностей, %			
	1-й цикл	2-й цикл	3-й цикл, Key 1	3-й цикл, Key 2
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

Для линейных показателей даже при отобранных S-блоках с нелинейностью 128–104 = 24 имеем $LP_{\max}^{\pi} = 2^{-4,83}$. Уравнение $2^{-121} = 2^{k-1}(2^{-4,8})^k$ приводит к результату $k_{\min} = 31,58$ и, следовательно, для прихода шифра Калина к состоянию случайной подстановки по линейным показателям, как и для шифра Rijndael, необходимо четыре цикла!

Второе предложение. Для 256-битного шифра снова используется решение, аналогичное предложенному при построении усовершенствованного шифра Rijndael [3] (см. рис. 3), только теперь в инволютивной операции участвуют 64-битные сегменты входного блока данных (после операции забеливания). Можно убедиться, что при такой схеме подключения к первому циклу минимальное число активизируемых S-блоков первого цикла и в этом случае равно трем. В результате минимальное число S-блоков, которые активизируются на первом и втором циклах, с большой вероятностью всегда оказывается больше или равным 35. Тогда на трех циклах гарантированно активизируются, как правило, 67 S-блоков. В соответствии с данными, приведенными в [9], шифр становится случайной подстановкой и по линейным, и по дифференциальным показателям за три цикла, причем, как будет показано далее, и при S-блоках случайного типа.

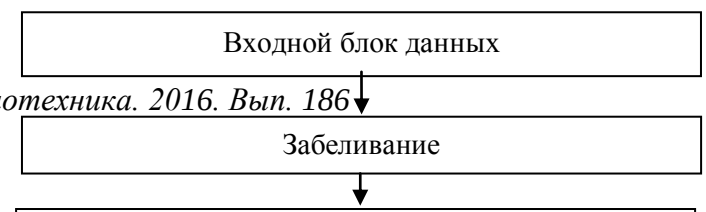

Рис. 3

Рис. 3

Третье предложение. Для 512-битного шифра можно воспользоваться предыдущим решением, только теперь для каждого 128-битного полублока применим свое инволютивное преобразование, как это показано на рис. 4.

Для усовершенствованной Калины-512 минимальное число активизируемых S-блоков на трех первых циклах равно 131.

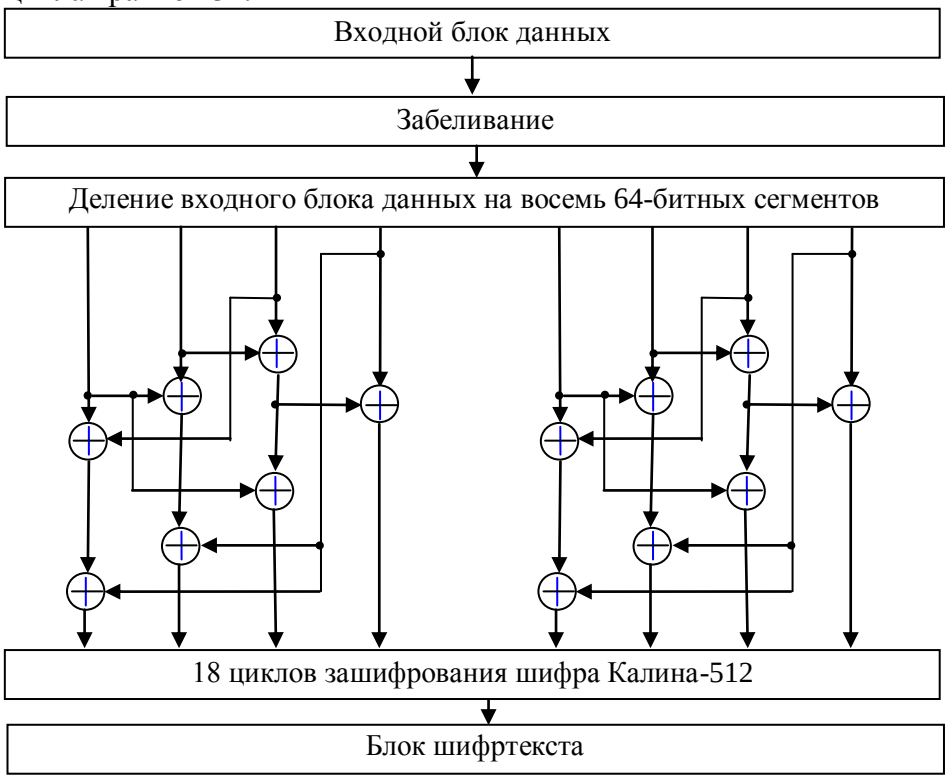

Рис. 4

2. Использование случайных S-блоков

128-битный шифр Калина. Оценим перспективы использования в 128-битном усовершенствованном шифре Калина случайных S-блоков. Методика выполнения расчетов представлена в работе [8]. В случае на первом цикле ожидается активизация одним байтом входа минимум трех S-блоков первого цикла, причем эти S-блоки будут размещаться в разных колонках матрицы состояний. Поэтому получается, что на втором и третьем циклах будут активизироваться с большой вероятностью сразу все 16 S-блоков каждого из циклов (по восемь в каждой колонке). В результате на трех циклах будет активизироваться более 35 S-блоков. В табл. 5 представлены результаты расчетов числа переходов разного типа в 35 строках дифференциальной таблицы байтовой случайной подстановки.

Таблица 5

Значение перехода таблицы	Число переходов дифференциальной таблицы	Число переходов в строке	Число переходов в 35 строках
12	1	0,003906	0,19
10	10	0,039065	1,367
8	104	0,40625	14,21
6	830	3,24218	113,48

Из представленных результатов следует, что 35 активных S-блоков (активных переходов) можно выбрать при случайных входах в S-блоки на основе использования:

- одного перехода со значением максимума в строке равным 10;
– четырнадцати переходов со значением максимума в строке равным 8;
- двадцати переходов со значениями максимумов равными 6 (используются максимально вероятные переходы). Всего 35 переходов (35 активных S-блоков).

Вычисления для 35 S-блоков в этом случае приводят к результату:

$$\left(\frac{12}{256}\right)\times\left(\frac{10}{256}\right)^{14}\times\left(\frac{8}{256}\right)^{20}=2^{-169}.$$

Это означает, что и случайные S-блоки по дифференциальным показателям обеспечивают с большим запасом приход шифра Калина за три цикла к состоянию случайной подстановки.

Приведем распределение переходов для смещений линейной аппроксимационной таблицы. В общее число переходов здесь входят и положительные и отрицательные смещения. Пользуясь результатами работы [8], можем рассчитать числа переходов разного типа в 35 строках линейной аппроксимационной таблицы случайной подстановки, итоги расчетов которых представлены в табл. 6.

Будем считать, что за счет введения цикловых подключей входы в S-блоки – случайные и статистически независимые.

Из табл. 6 следует, что для 35 активных S-блоков при использовании в них максимально вероятных переходов можно ожидать при случайных входах в случайные S-блоки:

- один переход со значением 30;
- четыре перехода со значением 28;
- девять переходов со значением 26;
- двадцать один переход со значением 24.

Полагая далее, что строки в S-блок выбираются из всего множества 256 строк, при этом переходы по S-блокам идут в произвольном порядке и осуществляются по наиболее вероятному пути, можем оценить вероятность прихода шифра к состоянию случайной подстановки со случайными S-блоками. Вычисления для значения $k = 35$ приводят к результату:

$$2^{34}\times\left(\frac{30}{128}\right)^2\times\left(\left(\frac{28}{128}\right)^2\right)^4\times 2^{34}\times\left(\frac{30}{128}\right)^2\times\left(\left(\frac{28}{128}\right)^2\right)^4\times\left(\left(\frac{26}{128}\right)^2\right)^9\times\left(\left(\frac{24}{128}\right)^2\right)^{21}=2^{-130}.$$

Таблица 6

Значение перехода	Число переходов в таблице ЛАТ	Число переходов в строке таблицы ЛАТ	Число переходов в 35 случайно взятых строках таблицы ЛАТ
±34	1,998	0,0078	0,273
±32	4	0,0156	0,546
±30	10	0,0392	1,372
±28	28	0,1098	3,843
±26	65	0,2588	9,058
±24	146	0,572	20,02
±22	298	1,164	40,74

Получается, что 35 случайных S-блоков достаточно для того, чтобы шифр стал случайной подстановкой (расчетное значение максимума линейной вероятности для 128-битного шифра есть 2^{-120}). Таким образом, можно считать шифр при трех циклах зашифрования гарантированно стойким и против атак линейного криптоанализа.

256 битный шифр. В соответствии с результатами табл. 3 в этом случае на трех циклах ожидается активизация одним байтом входа минимум двух S-блоков, причем эти S-блоки будут размещаться в разных колонках матрицы состояний. Поэтому получается, что на втором и третьем циклах будут активизироваться с большой вероятностью сразу все 32 S-блока каждого цикла. На трех циклах будут активизироваться минимум 68 S-блоков.

В табл. 7 представлены результаты расчетов числа переходов разного типа в 68 строках дифференциальной таблицы байтовой случайной подстановки. Из представленных результатов следует, что 68 активных S-блоков (активных переходов) можно выбрать при случайных входах в S-блоки на основе использования:

- трех переходов со значениями 10;
- двадцати восьми переходов со значениями 8;
- тридцати семи переходов со значениями 6;

(опять используются максимально вероятные переходы). Всего 68 переходов (68 активных S-блоков). Вычисления в этом случае приводят к результату:

$$\left(\frac{10}{256}\right)^3 \times \left(\frac{8}{256}\right)^{28} \times \left(\frac{6}{256}\right)^{37} = 2^{-354}.$$

Таблица 7

Значение перехода таблицы	Число переходов дифференциальной таблицы	Число переходов в строке	Число переходов в 68 строках
12	1	0,003906	0,2656
10	10	0,039065	2,656
8	104	0,40625	27,625
6	830	3,24218	220,468

Это означает, что и случайные S-блоки по дифференциальным показателям обеспечивают приход шифра Калина за три цикла к состоянию случайной подстановки.

Рассмотрим теперь переходы в таблице ЛАТ.

Опять будем считать, что за счет введения цикловых подключей входы в S-блоки будут случайными и статистически независимыми.

В табл. 8 представлены результаты оценки числа переходов и их значений в 68 случайно взятых строках таблицы ЛАТ. Из результатов следует, что для 68 активных S-блоков при использовании в них максимально вероятных переходов можно ожидать при случайных входах в случайные S-блоки:

- один переход со значением 32;
- три перехода со значением 30;
- семь переходов со значением 28;
- семнадцать переходов со значением 26;
- сорок переходов со значением 24

(два S-блока первого цикла могут быть взяты с максимально возможным значением перехода 34).

Таблица 8

Значение перехода	Число переходов в таблице ЛАТ	Число переходов в строке таблицы ЛАТ	Число переходов в 68 случайно взятых строках таблицы ЛАТ
±34	1,998	0,0078	0,5304
±32	4	0,0156	1,0608
±30	10	0,0392	2,6656
±28	28	0,1098	7,4664
±26	65	0,2588	17,5984
±24	146	0,572	38,896
±22	298	1,164	79,152

Полагая далее, что строки в S-блок выбираются из всего множества 256 строк равновероятно, при этом переходы по S-блокам идут в произвольном порядке и осуществляются по наиболее вероятному пути, можем оценить вероятность прихода шифра к состоянию случайной подстановки со случайными S-блоками. Вычисления для 68 активных S-блоков приводят к результату:

$$2^{67}\times\left(\frac{32}{128}\right)^2\left(\left(\frac{30}{128}\right)^2\right)^3\times\left(\left(\frac{28}{128}\right)^2\right)^7\times\left(\left(\frac{26}{128}\right)^2\right)^{17}\times\left(\left(\frac{24}{128}\right)^2\right)^{40}=2^{-252}.$$

И здесь 68 случайных S-блоков достаточно для того, чтобы шифр стал случайной подстановкой (максимальная дифференциальная вероятность для 256-битного шифра Калина > 2^{-250}). Таким образом, можно считать, что шифр Калина-256 при трех циклах зашифрования является гарантированно стойким против атак линейного криптоанализа и при случайных S-блоках.

512 битный шифр. В этом случае на трех циклах ожидается активизация минимум 130 S-блоков. В табл. 9 представлены результаты расчетов числа переходов разного типа в 130 строках дифференциальной таблицы байтовой случайной подстановки.

Таблица 9

Значение перехода таблицы	Число переходов дифференциальной таблицы	Число переходов в строке	Число переходов в 130 строках
12	1	0,003906	0,5
10	10	0,039065	5,078
8	104	0,40625	52,81
6	830	3,24218	423,48

Из представленных результатов следует, что 130 активных S-блоков (активных переходов) можно выбрать при случайных входах в S-блоки на основе использования:

- пяти переходов со значением 10;
- пятидесяти трех перехода со значением 8;
- семидесяти двух переходов со значением 6;

(используются максимально вероятные переходы). Всего 130 переходов (130 активных S-блоков). Вычисления в этом случае приводят к результату:

$$\left(\frac{10}{256}\right)^5\times\left(\frac{8}{256}\right)^{53}\times\left(\frac{6}{256}\right)^{72}=2^{-678}.$$

Это означает, что случайные S-блоки по дифференциальным показателям с большим запасом обеспечивают приход шифра Калина за три цикла к состоянию случайной подстановки (для 512-битной версии шифра значение максимума дифференциальной вероятности находится на уровне более 2^{-500}).

Приведем распределение переходов для смещений линейной аппроксимационной таблицы. В общее число переходов здесь входят и положительные, и отрицательные смещения. Пользуясь результатами работы [8], можем рассчитать числа переходов разного типа в 130 строках линейной аппроксимационной таблицы случайной подстановки, итоги расчетов которых представлены в табл. 10.

Таблица 10

Значение перехода	Число переходов в таблице ЛАТ	Число переходов в строке таблицы ЛАТ	Число переходов в 130 случайно взятых строках таблицы ЛАТ
±34	1,998	0,0078	1,014
±32	4	0,0156	2,028
±30	10	0,0392	5,096
±28	28	0,1098	14,274
±26	65	0,2588	33,644
±24	146	0,572	74,36
±22	298	1,164	151,32

Будем считать, что за счет введения цикловых подключей входы в S-блоки будут случайными и статистически независимыми.

В таблице представлены результаты оценки числа переходов и их значений в 130 случайно взятых строках таблицы ЛАТ. Из результатов следует, что для 130 активных S-блоков при использовании в них максимально вероятных переходов можно ожидать при случайных входах в случайные S-блоки:

- один переход со значением 34;
- два перехода со значением 32;
- пять переход со значением 30;
- четырнадцать переходов со значением 28;
- тридцать четыре перехода со значением 26;
- семьдесят четыре перехода со значением 24

(S-блоки первого цикла могут быть взяты с максимально возможным значением перехода 34).

Полагая, что строки в S-блок выбираются из всего множества 256 строк, при этом переходы по S-блокам идут в произвольном порядке и осуществляются по наиболее вероятному пути, можем оценить вероятность прихода шифра к состоянию случайной подстановки со случайными S-блоками. Вычисления для значения $k = 130$ приводят к результату:

$$2^{129}\times\left(\frac{34}{128}\right)^2\times\left(\left(\frac{32}{128}\right)^2\right)^2\left(\left(\frac{30}{128}\right)^2\right)^5\times\left(\left(\frac{28}{128}\right)^2\right)^{14}\times\left(\left(\frac{26}{128}\right)^2\right)^{34}\times\left(\left(\frac{24}{128}\right)^2\right)^{74}=2^{-479}.$$

Здесь 130 случайных S-блоков недостаточно, чтобы шифр стал случайной подстановкой. Однако линейная вероятность 2^{-479} является достаточной, чтобы шифр считать стойким. Таким образом, можно считать 512-битный шифр при трех циклах зашифрования гарантированно стойким и против атак линейного криптоанализа.

Напомним, что шифр Калина тоже приходит к состоянию случайной подстановки по дифференциальным и линейным показателям на третьем и четвертом циклах зашифрования, но при специально отобранных S-блоках.

3. Оценка числа сменных узлов замены

Теперь нас будет интересовать число случайных подстановок, которые можно использовать в качестве узлов замены в шифре Калина.

Приведем результаты построения законов распределения и экспериментальные данные для максимумов переходов дифференциальных таблиц и смещений таблиц линейных аппроксимаций случайных байтовых подстановок [10]. Они представлены в табл. 11 и 12.

Таблица 11

$k^*(X_1, X_2)$	Pr(k^*)	Расчетное значение	Эксперимент
8	0,00004	0,01	0
10 (10,8)	0,368 – 0,00004 = 0,368	94	111
12 (12,10)	0,905 – 0,368 = 0,537	137	130
14 (14, 12)	0,9901 – 0,905 = 0,008	22	15
16 (16,14)	0,9967 – 0,9901 = 0,0066	1,71	1
18 (18,16)	0,9999– 0,9967 = 0,0032	0,819	0

Таблица 12

$k^*(X_1, X_2)$	Pr(k^*)	Число значений по расчету	Эксперимент
< 26	$3.41\ 10^{-7}$	0	0
28 (28,26)	$5{,}6\ 10^{-4} – 3{,}4110^{-7} = 5{,}6\ 10^{-4}$	0,14	0
30 (30,28)	$0{,}064 – 5{,}6\ 10^{-4} = 0{,}0638$	16	14
32 (32,30)	0,368–0,064 = 0,304	78	67
34 (34,32)	0,692 – 0,304 = 0,388	99	108
36 (36,34)	0,874 – 0,692 = 0,181	46	37
38(38,36)	0,9518 – 0,874 = 0,078	19	22
40 (40,38)	0,9821 – 0,9518 = 0,03	8	8
42 (42,40)	0,9933 – 0,9821 = 0,011	3	1
44 (44,42)	0,9975 – 0,9973 = 0,00028	0,07	0

Видно, что расчетные значения практически повторяют значения, полученные экспериментальным путем. Как следует из представленных результатов, основная масса подстановок по значениям максимумов переходов повторяет теоретические (расчетные) показатели случайных подстановок [9]. Это значения для дифференциальных таблиц подстановок равны 6-8, а для таблиц линейных аппроксимаций – 32-34. Имеется также небольшая часть переходов с минимальными (предельными) значениями максимумов и со значениями максимумов, увеличенными до 10.

В табл. 13, заимствованной из работы [10], приведено распределение максимумов дифференциальных (строки) и линейных (колонки) вероятностей для всех 16! полубайтовых подстановок (для байтовых подстановок такой эксперимент вычислительно нереализуем).

Следует отметить, что даже усеченное распределение байтовых подстановок (табл. 11 и 12) практически повторяет распределение максимальных переходов для основной массы полубайтовых подстановок (табл. 13).

Из таблицы видно, что основная масса, 54,7155 % всех S-блоков, имеет дифференциальную границу $p < 3/8$ и линейную границу $\varepsilon < 3/8$, при этом:

$p = 1/4$ соответствует значению перехода полубайтовой подстановки равному 4;

$p = 3/8$ соответствует значению перехода полубайтовой подстановки равному 6;

$p = 1/2$ соответствует значению перехода полубайтовой подстановки равному 8;

$p = 5/8$ соответствует значению перехода полубайтовой подстановки равному 10;

$p = 3/4$ соответствует значению перехода полубайтовой подстановки равному 12;

В [10] смещение определяется как

$$\varepsilon = \mathrm{abs}\left(\frac{n}{|S|} - \frac{1}{2}\right).$$

Таблица 13

LC →	$\epsilon \le 1/4$		$\epsilon \le 3/8$		$\epsilon \le 1/2$	
DC ↓	n	%	n	%	n	%
$p \le 1/4$	749123665920	3.5804	326998425600	1.5629	0	0.0000
$p \le 3/8$	1040449536000	4.9728	11448247910400	54.7166	118908518400	0.5683
$p \le 1/2$	52022476800	0.2486	5812644741120	27.7814	330249830400	1.5784
$p \le 5/8$	0	0.0000	728314675200	3.4810	193458585600	0.9246
$p \le 3/4$	0	0.0000	52022476800	0.2486	68098867200	0.3255
$p \le 1$	0	0.0000	309657600	0.0015	1940520960	0.0093

Это значит, что:

ε = 1/4 соответствует смещению таблицы полубайтовой подстановки равному 12 (для байтовой подстановки это будет значение меньшее 30);

ε = 3/8 соответствует смещению таблицы полубайтовой подстановки равному 14 (для байтовой подстановки это значение близкое к 34);

ε = 1/2 соответствует смещению таблицы байтовой подстановки равному 16 (для байтовой подстановки это значение, превышающее 42).

Видно, что результаты экспериментов хорошо согласуются с данными табл. 13. Здесь наиболее вероятным значением максимума является значение 6.

Для байтовых подстановок наиболее вероятным значением максимума является значение 12. И относительно этого значения выстраиваются, практически повторяя закон распределения максимумов полубайтовых подстановок, остальные значения.

Результаты свидетельствуют, что рассматриваемая версия генератора “случайных” подстановок пригодна для формирования мастер-ключей.

При необходимости отсева вырожденных подстановок можно выполнять проверку сгенерированных случайно подстановок по значениям максимумов дифференциальных и линейных переходов. Эти значения максимумов должны находиться в пределах 4-10 для дифференциальных показателей и 28-34 – для линейных показателей.

Предложенные конструкции шифров ввиду улучшенных показателей их прихода к случайным постановкам допускают без потери стойкости уменьшение числа цикловых преобразований до 12 и меньше (в зависимости от длины шифруемого блока и ключа).

Выводы

Представленные предложения по усовершенствованию шифра Калина позволяют использовать в шифре в качестве узлов замены случайные S-блоки без снижения показателей стойкости.

Подходящими для построения узлов замены в этом случае являются более половины всего множества подстановок. Для байтовых подстановок это более 2^{1683} узлов замены. Если в шифре используются разные подстановки, то их ансамбль оценивается числом 2^{6736} для четырех разных S-блоков и 2^{13464} – для восьми разных подстановок.

Заметим, что в Калине используются специально отобранные S-блоки. Они имеют δ-равномерность равную четырем (p = ¼), нелинейность равную 128 – 104 = 24 (ε < ¼), алгебраическую степень менее семи и ограниченный алгебраический иммунитет. Из табл. 11 и 12 следует, что вероятность их получения (отбора) только по допустимым значениям дифференциальных переходов и смещений намного меньше 10^{-40} (< 2^{-23}), не говоря уже о других ограничениях (даже с учетом взаимозависимости этих показателей таких подстановок оказывается существенно меньше).

В заключение можно отметить разработку – шифр ШУП-1 [2], построенный в соответствии с новой концепцией проектирования блочных симметричных шифров [1]. Этот шифр сразу ориентирован на использование случайных S-блоков. Он становится случайной подстановкой уже на двух первых циклах зашифрования (а ШУП-2 становится случайной подстановкой уже с первого цикла). За счет улучшения динамических показателей прихода к

случайной подстановке при его построении использовано восемь циклов шифрования, что, в свою очередь, позволило добиться дополнительного повышения быстродействия конструкции (не говоря уже о возможности реализации в этом шифре конвейерной обработки данных).

Список литературы: 1. *Долгов, В.И.* Новая концепция проектирования блочных симметричных шифров / В.И. Долгов, И.В. Лисицкая, К.Е Лисицкий // Радиотехника. – 2016. – Вип.186. – 132-152. 2. *Пат. 111547* Україна, МПК (2016.01) G09C 1/00 H04L 9/06 (2006.01). Спосіб криптографічного перетворення двійкових даних (варіанти) / І.Д. Горбенко, В.І. Долгов, І.В. Лисицька та інші (Україна) ; заявник АО ІІТ м. Харків. № a201500942 ; заявл. 06.02.2015 ; опубл. 10.05.2016. Бюл. № 9. – 20 с. 3. *Лисицкий, К.Е.* Новое усовершенствование Rijndael-я / К.Е. Лисицкий // Наук.-практ. конф. "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" / Київ. нац. ун-т імені Тараса Шевченка. 10–11 апреля 2016 г. – С.51. 4. *Долгов, В.И.* Методология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа : монография / В.И. Долгов, И.В. Лисицкая. Харьков : Форт, 2013. – 420 с. 5. *Стандарт* блочного симметричного преобразования ДСТУ 7624:2014. – [Чинний від 01.06.2015]. .– К. : Держстандарт України, 2014. – 111 с. (Национальний стандарт України). 6. *Горбенко, І.Д.* Принципи побудування та властивості блокового симетричного шифру "Калина" / І.Д. Горбенко, В.І. Долгов, Р.В. Олійников та інші // Прикладная радиоэлектроника. – 2007. – Т. 6, №2. – С. 147-157. 7. *Пат. 111448* Україна, МПК H04L 29/14 (2006.01) H04L 9/14 (2006.01) H04L 9/06 (2006.01). Спосіб криптографічного перетворення двійкових даних / І.Д. Горбенко, В.І. Долгов, І.В. Лисицька та інші (Україна) ; заявник АО ІІТ м. Харків. № a201503976 ; заявл. 25.04.2015; опубл. 25.04.2016. Бюл. № 8 – 20 с. 8. *Горбенко, И.Д.* О динамике прихода блочных симметричных шифров к случайной подстановке / И.Д. Горбенко, Е.К. Лисицкий // Радиотехника. – 2014. – Вип.176. – С. 27-39. 9. *Лисицкая, И.В*. О криптографической значимости схем разворачивания ключей в обеспечении стойкости блочных симметричных шифров к атакам линейного и дифференциального криптоанализа / И.В. Лисицкая, А.А. Настенко К.Е. Лисицкий // Радиоэлектроника и информатика. – 2012. – № 3(58). – С. 56-65. 10. *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. 11. *Лисицкий, К.Е* Уточненная математическая модель случайной подстановки / К.Е. Лисицкий, Е.Д. Мельничук / Автоматизированные системы управления и приборы автоматики. – 2013. – Вып. 162. – С. 22-28.

Харьковский национальный
университет имени В.Н. Каразина

Поступила в редколлегию 17.09.2016