

## О СТОЙКОСТИ БЛОЧНЫХ ШИФРОВ С RIJNDAEL-ПОДОБНЫМИ ПРЕОБРАЗОВАНИЯМИ К ИНТЕГРАЛЬНЫМ АТАКАМ

В.И. РУЖЕНЦЕВ

Работа посвящена исследованию особенностей организации интегральных атак на различные варианты шифров с rijndael-подобными преобразованиями, выполняется сравнение этих шифров по стойкости к интегральному криптоанализу, уточняются опубликованные ранее результаты относительно стойкости блочных шифров.

*Ключевые слова:* блочный шифр, интегральный криптоанализ, rijndael-подобные преобразования,  $n$ -цикловый интеграл.

### ВВЕДЕНИЕ

Интегральный криптоанализ является одним из наиболее эффективных видов нападения на самый распространенный в мире шифр rijndael [1] (и его вариант – AES [2]) с уменьшенным количеством циклов. Распространенность данного шифра привела также к частому использованию его элементов в других шифрах. Так, например, все алгоритмы шифрования, которые были представлены в национальном конкурсе блочных симметричных шифров [3], использовали rijndael-подобные преобразования. В наших работах [4-6] проводился анализ возможности организации, в том числе, и интегральной атаки на некоторые из шифров – участников конкурса [3]. Целью настоящей работы является, с одной стороны, изложение особенностей организации интегральных атак на различные варианты шифров с rijndael-подобными преобразованиями, с другой стороны, сравнение этих шифров по стойкости к интегральному криптоанализу.

### 1. ОБЩАЯ ХАРАКТЕРИСТИКА АТАКИ. ИСПОЛЬЗУЕМЫЕ ОБОЗНАЧЕНИЯ

Интегральная атака на блочные симметричные шифры относится к классу атак на цикловую функцию, и для ее реализации необходимо иметь достаточное множество криптограмм, полученных при зашифровании подобранных открытых текстов на одном и том же секретном ключе.

Интегральной атака названа, потому что в атаке рассматривается прохождение через преобразования шифра суммы состояний. Здесь под различными состояниями понимаются некоторые промежуточные значения блоков преобразуемых данных в процессе их зашифрования. Подобно тому, как в дифференциальном криптоанализе производится “транспортирование” разности через преобразования шифра, в данной атаке через циклы шифра проводится значение суммы состояний из некоторого множества.

Если имеется возможность с высокой вероятностью предсказать значение некоторых битов суммы состояний после  $r$  циклов шифрования, то это означает, что может быть организована интегральная атака на  $(r+1)$ -цикловый шифр. В ходе атаки перебираются возможные подключи

последнего цикла и для каждого варианта производится дешифрование одного цикла для всего множества имеющихся криптограмм. Если в результате суммирования информационных блоков, полученных при одноцикловом дешифровании, на известных позициях будет получено нужное значение, то с высокой вероятностью проверяемая часть подключа последнего цикла является верной. Более подробно особенности организации этого вида атак изложены в [7].

Для дальнейшего описания особенностей организации интегральных атак на различные шифры удобно будет воспользоваться обозначениями, введенными в работе [7]. Интеграл первого порядка обычно состоит из  $2^8$  состояний. Будем использовать следующие обозначения для отдельных байтов:

A – байт «all» - в каждом из состояний на этой позиции уникальное, отличное от остальных состояний значение.

C – байт «constant» - в каждом из состояний на этой позиции идентичное значение.

S – байт «sum» - сумма по XOR значений на этой позиции для всех состояний равно 0.

? – про байт ничего не известно.

Интеграл порядка  $d$  состоит из  $2^{8d}$  состояний. Байты «C», «S» и «?» имеют прежние значения. Байты «A» имеют верхний и нижний индексы: верхний обозначает порядок интеграла, нижний индекс указывает на то, что конкатенация всех слов (байтов) с одинаковым нижним индексом будет иметь уникальное  $8d$ -битное значение для каждого состояния. Если все  $d$  таких слова (байта) стоят в блоке рядом, то будем обозначать их на рисунках одной общей ячейкой, обозначенной символом «A».

Относительно интегралов разных порядков следует заметить, что при равном числе циклов более эффективен интеграл меньшего порядка, так как его использование в атаке требует меньших вычислительных затрат. Поэтому в дальнейшем для анализируемых шифров будем приводить лишь самые эффективные из найденных интегралов, то есть такие, которые покрывают максимальное количество циклов и обладают минимальным порядком.

## 2. ИНТЕГРАЛЬНЫЕ СВОЙСТВА RIJNDAEL-ПОДОБНЫХ ПРЕОБРАЗОВАНИЙ

Напомним как «А», «С» и «S» байты проходят через основные rijndael-подобные преобразования. ByteSub или подстановка 8 в 8 битов не меняет байты «А» и «С». Сложение с ключом по XOR не меняет байты «А», «С» и «S». Основные правила прохождения через MixColumn представлены на рис. 1.

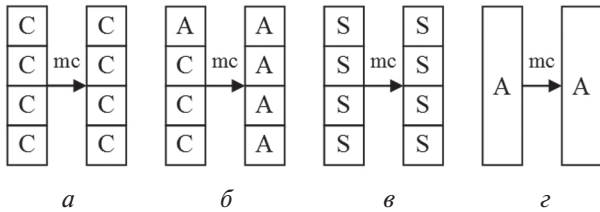


Рис. 1

При этом следует заметить, что поскольку байты «А» и «С» обладают свойствами байтов «S», то правило на рис. 1, в будет применимо, например, и для входной комбинации AACС; результат будет – SSSS. Правило на рис. 1, z показывает, что если на вход MixColumn подавать все возможные 32-битные значения, то все возможные значения будут получены и на выходе.

В табл. 1 представлены известные правила изменения байтов при прохождении через операцию XOR, которая часто встречается в схемах Фейстеля и схемах Лея-Мессии.

Таблица 1

ΞOP	A	X	Σ	?
A	Σ	A	Σ	?
X	A	X	Σ	?
Σ	Σ	Σ	Σ	?
?	?	?	?	?

В качестве базового циклового преобразования для шифров будем использовать преобразование SL, схема которого представлена на рис. 2.

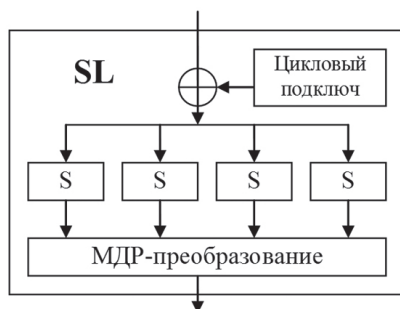


Рис. 2

## 3. АНАЛИЗ ШИФРОВ, ИСПОЛЬЗУЮЩИХ SL-ПРЕОБРАЗОВАНИЕ

### Схема SPN.

Рассмотрим шифр с SL-преобразованием в качестве цикловой функции.

В SPN схеме одно SL-преобразование следует за другим. В такой схеме имеется 2-цикловый

интеграл 1-го порядка, на входе которого один активный байт, а на выходе все байты «S» (см. рис. 3).

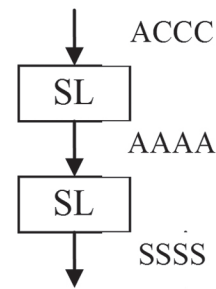


Рис. 3

Такой интеграл позволяет организовать атаку на 3-цикловый шифр.

Интегралы более высоких порядков для данной схемы преобразований не будут более эффективными, так как интеграл 4-го порядка потребует  $2^{32}$  открытых текстов, а это есть полное множество открытых текстов – в этом случае эффективнее словарная атака (построение «словаря» для полного множества входных текстов).

### Схема Фейстеля.

Интегральные атаки на фейстель-подобные шифры описаны в работах [4,8].

На рис. 4 представлен 4-цикловый интеграл 1-го порядка, который позволяет организовать атаку на такой шифр с 5 циклами.

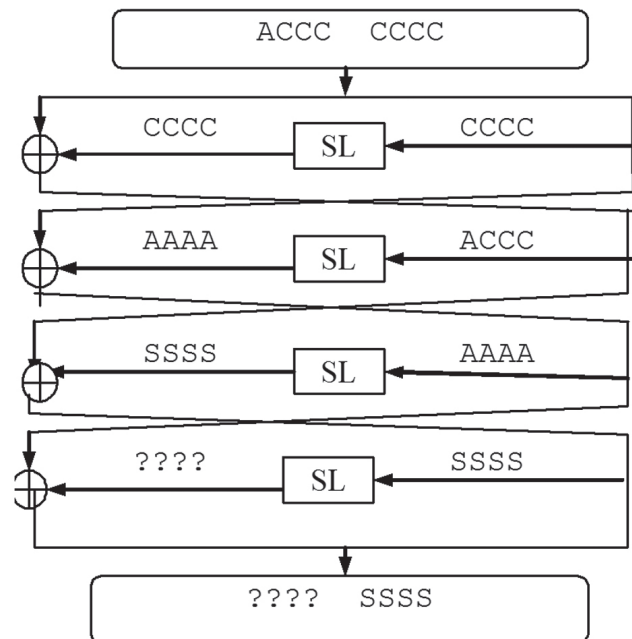


Рис. 4

Интегралов более высоких порядков, покрывающих большее число циклов найдено не было.

**Схема Лея-Мессии.** Особенности организации атак на шифры с использованием схемы Лея-Мессии обсуждаются в [5,9].

На рис. 5 представлен 2-цикловый интеграл, который позволяет организовать атаку на такой шифр с 3 циклами.

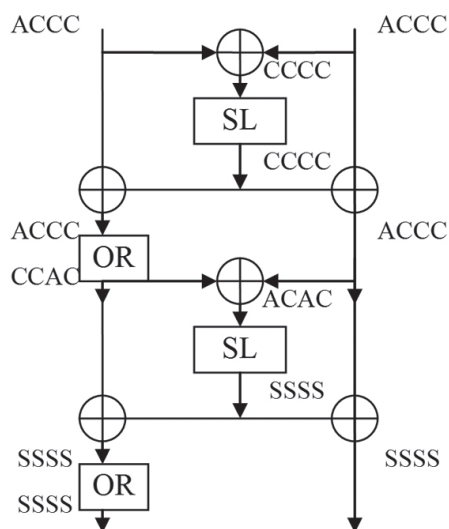


Рис. 5

В рассматриваемом шифре перед первым циклом нет никаких операций, поэтому есть возможность обхода правила сложения по XOR байтов «А» из табл. 1. Подавая на позиции «А» в левом и правом полублоке синхронно одинаковые значения можно инициировать получение при сложении байта «С», что и изображено на рис. 5.

В шифре «Мухомор», который анализировался в [5], присутствует начальное забеливание, что делает описанный интеграл неприменимым. Наиболее эффективными для данного шифра остаются интегралы, представленные в [5].

Интегралов более высоких порядков, покрывающих большее число циклов для рассматриваемого варианта шифра, найдено не было.

Учитывая то, что по сравнению со схемой SPN схемы Фейстеля и Лея-Месси имеют в 2 раза больший размер блока, среди рассмотренных вариантов использования SL-преобразования предпочтительнее остальных выглядит схема Лея-Месси. Главная причина этого, на наш взгляд, заключается в достаточно большом количестве операций XOR между подблоками (3 в одном цикле плюс 1 в операции ORT), что затрудняет прохождение через преобразования байтов «А».

#### 4. ВАРИАНТЫ СХЕМЫ SPN

В этом подразделе уточняются представленные в работе [6] данные о стойкости к интегральной атаке rijndael-подобных шифров, построенных с использованием предложенного в [10] подхода. К таким шифрам, в частности, относится алгоритм «Калина» [11].

Кратко изложим суть предложенного в [10] подхода.

Анализ известных БСШ показал, что существуют два способа использования МДР-преобразований при построении операций рассеивания SPN-шифров. При первом способе используется МДР-преобразование, которое покрывает весь блок. В этом случае блок

представляется в виде вектора, а преобразование заключается в умножении этого вектора на квадратную МДР-матрицу соответствующего размера. Схема такого преобразования для размера блока  $m$  байтов представлена на рис. 6, а. Таким строением линейных преобразований обладают шифры Shark, Khazad и рассмотренные в разделе 3 варианты SPN шифров. В соответствии с основным свойством МДР-преобразований, каждая 2-цикловая дифференциальная или линейная характеристика для этих шифров будет содержать не менее  $m+1$  активных S-блоков. Основным недостатком данного способа построения линейных преобразований является большой размер используемой МДР-матрицы, что обычно приводит к повышенной сложности вычислений.

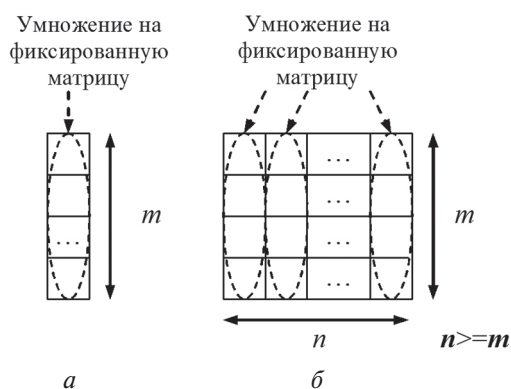


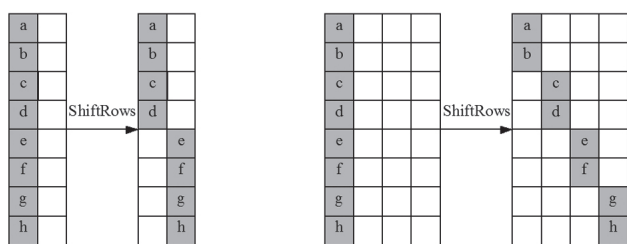
Рис. 6. Известные схемы построения линейных операций с использованием МДР-преобразований

Во втором случае используется «rijndael-подобная» структура линейных преобразований, то есть, блок разбивается на  $n$  векторов по  $m$  байтов каждый (общий размер блока  $n \times m$  байтов), при чем,  $n$  больше или равен  $m$  (см. рис. 6, б).

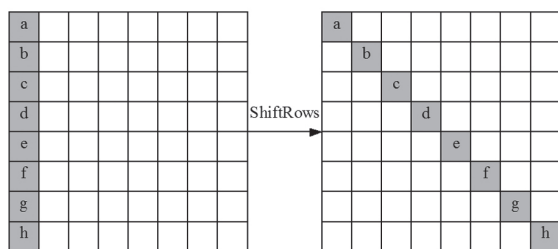
Линейное преобразование заключается в том, что каждый  $m$ -байтный вектор, называемый колонкой, умножается на МДР-матрицу размером  $m \times m$  байтов, после чего выполняется байтовая перестановка, в ходе которой байты каждой колонки распределяются по одному байту в каждую колонку. Аналог первой части операции рассеивания – процедура MixColumns в Rijndael, аналог байтовой перестановки – процедура ShiftRows. Подобное строение линейных преобразований используется также в шифрах Square, Crypton, Anubis.

В [10] обсуждался вариант линейных преобразований, когда  $m \geq n$ . По такой схеме построены линейные преобразования шифра «Калина» [11]. В этом шифре  $m = 8$ ,  $n$  меняется от 2 до 8 в зависимости от размера блока. В ходе операции MixColumns выполняется умножение на фиксированную матрицу размером  $8 \times 8$  байтов, а порядок перестановки байтов в ходе операции ShiftRows представлен на рис. 7.

Уточнения касаются возможности организации интегральной атаки на варианты шифра с одним дополнительным циклом по сравнению с представленными в [6] результатами.



а – 128-битный блок      б – 256-битный блок



в – 512-битный блок

Рис. 7

По аналогии с 4-цикловым интегралом 4-го порядка для шифра Rijndael, предложенного в [12], для рассматриваемого шифра также существует 4-цикловый интеграл порядка равного количеству байтов в колонке. На вход подаются  $2^{64}$  состояний, которые имеют уникальное 64-битное значение в 8 байтах, отмеченных серым цветом в начальной позиции на рис. 8.

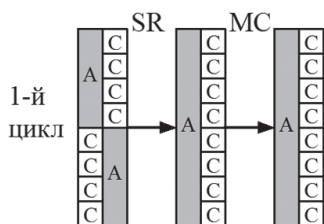


Рис. 8

Как видно из рис. 8, после операции ShiftRows эти 8 байтов оказываются в одной колонке. А в соответствии с правилом, представленным на рис. 1,г, после операции MixColumn будет получен такой же набор состояний. Этот набор состояний эквивалентен  $2^{32}$  наборам состояний, соответствующим входной позиции интеграла, который был предложен в [6] и представлен на рис. 9. (Каждый из  $2^{32}$  наборов состояний отличается от остальных значениями в четырех байтах «С» первой колонки.)

В итоге, мы получаем 4-цикловый интеграл 8-го порядка, который позволяет организовать атаку на 5-цикловый шифр с подобной структурой преобразований со сложностью около  $2^{65}$  операций шифрования.

Следует заметить, что подобный 4-цикловый интеграл 8-го порядка (порядок равен количеству байтов в колонке) существует и для других вариантов SPN шифров, использующих как схему линейных преобразований, представленную на рис. 6,б, так и схему, предложенную в работе [10].

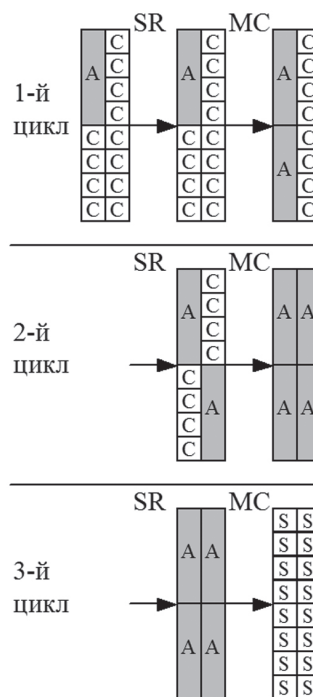


Рис. 9

## ВЫВОДЫ

В работе выполнено исследование стойкости к интегральному криптоанализу шифров с rijndael-подобными цикловыми преобразованиями построенных с использованием схем SPN, Фейстеля и Лея-Мессе. Сделан вывод о том, что более высокий уровень безопасности обеспечивает схема Лея-Мессе за счет большего, по сравнению с другими схемами, количества дополнительных операций XOR.

С учетом материалов работы [12], уточнены опубликованные ранее результаты о стойкости шифра «Калина» к интегральной атаке из [6]. Описано как может быть организована атака на варианты шифра с 5 циклами, что на 1 цикл больше, чем описано в [6]. Алгоритм с полным набором циклов обеспечивает защищенность от интегральной атаки.

## Литература

- [1] J. Daemen, V. Rijmen. AES Proposal Rijndael, AES Round 1 Technical Evaluation CD1: Documentation, National Institute of Standards and Technology, Aug 1998. See <http://www.nist.gov/aes>.
- [2] National Institute of Standards and Technology “Advanced encryption algorithm (AES) development.” // FIPS 197, U.S. Department of Commerce, Nov. 2001.
- [3] Офіційний ресурс департаменту спеціальних телекомунікаційних систем та захисту інформації: «Положення про проведення відкритого конкурсу криптографічних алгоритмів», 2006. Доступно по адресу <http://www.dststzi.gov.ua/dststzi/control/ru/publish/article/>.
- [4] Долгов В.И., Головашич С.А., Руженцев В.И. Криптостойкость шифра “Торнадо” // Радиотехника. 2003. № 134. С. 81-88.
- [5] Горбенко І.Д., Долгов В.І., Руженцев В.І. Олійников Р.В., Михайленко М.С. Криптостійкість шифру



“Мухомор” // Прикладна радіоелектроніка. Тематический випуск, посвящений проблемам забезпечення безпеки інформації. Харків. Том 6, №2, 2007 г. С. 186-194.

- [6] Горбенко І.Д., Долгов В.І., Руженцев В.І. Олійников Р.В., Михайленко М.С. Криптостійкість шифру “Калина” // Прикладна радіоелектроніка. Тематический випуск, посвящений проблемам забезпечення безпеки інформації. Харків. Том 6, №2, 2007 г. С. 217-229.
- [7] L. R. Knudsen. Integral Cryptanalysis, NESSIE internal report NES/DOC/UIB/WP5/015/1, 2001.
- [8] Y.-J. Li, W.-L. Wu, L.-T. Zhang, L. Zhang, Improved Integral Attacks on Reduced Round Camellia, IACR Eprint archive, 2011. available from <http://eprint.iacr.org/2011/163>.
- [9] W. Wenling, Z. Wentao, F. Dengguo, Improved Integral Cryptanalysis of FOX Block Cipher, IACR Eprint archive, 2005. available from <http://eprint.iacr.org/2005/292>.
- [10] V. Ruzhentsev, R. Oliynykov, Properties of Linear Transformations for Symmetric Block Ciphers on the basis of MDS-codes // Proceedings of the 6th International Conference on Network Architecture and Information System Security SAR-SSI 2011, pp. 193-196. La Rochelle, France.
- [11] Горбенко І.Д., Долгов В.І., Олійников Р.В., Руженцев В.І. та ін. Перспективний блоковий симетричний шифр “Калина” – основні положення та специфікація // Прикладна радіоелектроніка. Тематический випуск, посвящений проблемам забезпечення безпеки інформації. Харків. Том 6, №2, 2007 г. С. 195-208.
- [12] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting. Improved Cryptanalysis of Rijndael. FSE 2000, LNCS 1978, pp. 213-230, Springer-Verlag, 2001.

Поступила в редколлегию 26.03.2012



**Руженцев Виктор Игоревич**, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: симметричные криптоалгоритмы, криптоанализ.

УДК 621.391:519.2:519.7

**Про стійкість блокових шифрів з rijndael-подібними перетвореннями до інтегральних атак** / В.І. Руженцев // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 160–164.

Робота присвячена дослідженню особливостей організації інтегральних атак на різні варіанти шифрів з rijndael-подібними перетвореннями, виконується порівняння цих шифрів за рівнем стійкості до інтегрального криптоаналізу, уточнюються деякі з раніше опублікованих результатів стосовно стійкості блокових шифрів.

*Ключові слова:* блоковий шифр, інтегральний криптоаналіз, rijndael-подібні перетворення,  $n$ -цикловий інтеграл.

Табл. 1. Іл. 9. Бібліогр.: 12 назв.

UDC 621.391:519.2:519.7

**On the resistance of block ciphers with Rijndael-like transformations to integral attacks** / V.I. Ruzhentsev // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 160–164.

The paper is dedicated to studying peculiarities of organizing integral attacks on different variants of ciphers with rijndael-like transformations. Comparison of these ciphers resistance to integral cryptanalysis is performed. Some of the published earlier results about the ciphers resistance are refined.

*Key words:* block cipher, integral cryptanalysis, rijndael-like transformations,  $n$ -round integral.

Tab. 1. Fig. 9. Ref.: 12 items.