УДК 621. 391:519.2:519.7

КРИПТОГРАФИЧЕСКАЯ СТОЙКОСТЬ БЛОЧНЫХ ШИФРОВ ПРИ ИСПОЛЬЗОВАНИИ РАЗЛИЧНЫХ ОПЕРАЦИЙ СЛОЖЕНИЯ С ПОДКЛЮЧАМИ

В.И. РУЖЕНЦЕВ, В.В. СТУПАК

Исследуется криптографическая стойкость блочных симметричных шифров при использовании для введения секретности операций сложения по разным модулям. Рассматривается стойкость к дифференциальным, линейным, алгебраическим и другим атакам.

Ключевые слова: блочный симметричный шифр, криптографическая стойкость.

ВВЕДЕНИЕ

В соответствии с общеизвестными принципами Шеннона современные блочные симметричные шифры (БСШ) содержат операции перемешивания, рассеивания и операции введения секретности. В качестве операций перемешивания обычно используются подстановки, функции рассеивания возлагаются на линейные преобразования, а для введения секретности обычно используют сложение по XOR с подключом. Однако известны шифры, в которых для сложения с подключами используется не одна, а несколько операций сложения. К таким, например, относятся шифры семейства SAFER [1], а также представленные на национальный конкурс блочные шифры Калина [2], Лабиринт [3]. Целью данной работы является изложение результатов исследования криптографической стойкости блочных шифров при использовании в них операций сложения по разным модулям.

1. ОПИСАНИЕ РАССМАТРИВАЕМЫХ УМЕНЬШЕННЫХ МОДЕЛЕЙ

В рамках проведенных исследований рассматривались криптографические свойства фейстель-подобных и SPN блочных шифров с уменьшенным размером блока и ключа (8 или 16 битов). Целесообразность рассмотрения именно уменьшенных моделей шифров объясняется тем, что для изучения стойкости шифра к дифференциальной и линейной атаке следует, соответственно, оценивать вероятности полных дифференциалов и вероятности линейных корпусов – параметры, которые можно оценить только для шифра с небольшим размером блока. В качестве операций перемешивания и рассеивания были взяты преобразования, предложенные в [4] для уменьшенной версии шифра Rijndael. На рис. 1 и 2 схематически представлены преобразования, которые выполняются в рассматриваемых моделях фейстель-подобных и SPN шифров.

Исследованию криптографических свойств уменьшенных моделей блочных шифров посвящены и другие наши работы [5,6]. К основным особенностям предложенных уменьшенных моделей шифров следует отнести:

– размер блока 16 бит, размер ключа 8 или 16 бит;

– структура блока для SPN: 2 колонки по 2 4-битовых элемента;

– структура полублока для фейстель-подобного: 2 4-битовых элемента;

– умножение элементов каждой колонки на фиксированную МДР-матрицу размером 2 на 2 над $GF(2^4)$ (MixColumns);

– подстановка 4 в 4 бита (SubBytes);

– число ветвей активизации линейного преобразования MixColumns B = 3.

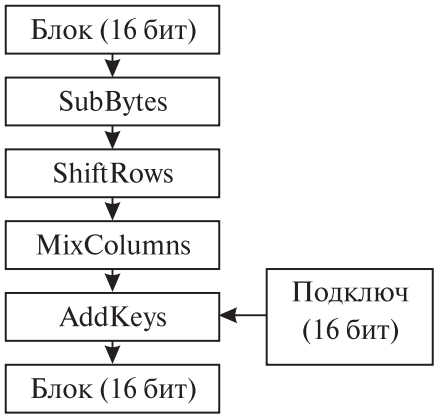

Рис. 1. Схема одного цикла SPN-шифра

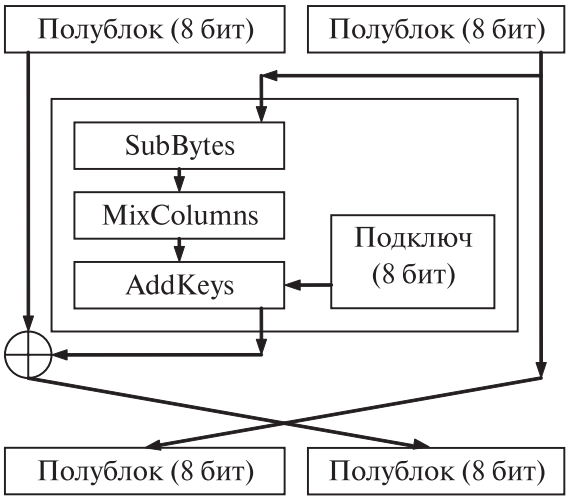

Рис. 2. Схема одного цикла фейстель-подобного шифра

2. СТОЙКОСТЬ К ДИФФЕРЕНЦИАЛЬНОМУ КРИПТОАНАЛИЗУ

Методика проверки точного критерия стойкости БСШ к дифференциальному криптоанализу сводится к оценке максимальных вероятностей дифференциалов. Для шифра с небольшим размером блока процесс поиска максимальных вероятностей дифференциалов похож на алгоритм построения таблиц разностей для подстановок, формируемых шифром при использовании различных ключей, и заключается в выполнении следующих шагов:

1. Перебираем значения ключа (100 значений).
2. Строим таблицу разности. Перебираем все значения входной разности (2^{16}).
3. Перебираем все значения одного из плайнтекстов (2^{16}).
4. Определяем выходную разность.
5. Определяем вероятности получения каждой выходной разности.
6. Определяем максимальную вероятность предсказания выходной разности
7. Определяем ожидаемое значение максимальной вероятности, усредняя значения, полученные на разных ключах.

Известны теоретические оценки ожидаемого значения максимальной вероятности дифференциала для случайной подстановки (см. представленную в этом же журнале статью «Дифференциальные свойства случайной подстановки»). Для случайной подстановки 16 в 16 битов математическое ожидание максимального значения в таблице разности составляет 19. Кроме того, из [6] известно, что для итеративного шифра при достижении некоторого количества циклов этот параметр перестает изменяться. Поэтому в итоговой таблице 1 приведено минимальное количество циклов, при котором шифры достигают теоретически ожидаемого максимума в таблице разности.

Таблица 1

Шифры (блок 16 битов)	Мин. число циклов для достижения теорет. ож. значения максим. вероятности дифференциала
SPN xor	5
SPN add	5
SPN add xor	5
FN xor	8
FN add	8
FN add xor	8

В табл. 1 и последующих таблицах использованы следующие обозначения:

SPN, FN – соответственно, SPN-шифр и фейстель-подобный шифр;

xor – в качестве операции сложения с подключом используется XOR;

add – в качестве операции сложения с подключом используется сложение по модулю 2^{16} для SPN и сложение по модулю 2^8 для фейстель-подобных шифров;

add xor – операции чередуются по циклам шифрования.

3. СТОЙКОСТЬ К ЛИНЕЙНОМУ КРИПТОАНАЛИЗУ

При оценке стойкости шифра к линейному криптоанализу следует проверять теоретический или точный критерий, то есть оценивать вероятности линейных корпусов (linear hull) (ЛК). Этот показатель может быть вычислен только для шифров с небольшим размером блока.

Процесс поиска ЛК, обладающего высокой вероятностью, похож на процесс построения таблицы линейных аппроксимаций для подстановки, образуемой шифром. Для получения значения вероятности ЛК необходимо произвести анализ вероятности ЛК для всех значений ключа, однако практическое решение такой задачи требует достаточно высоких вычислительных затрат. В ходе эксперимента вероятности ЛК оценивались только для одного ключа (все биты равны 0) и для ограниченного набора входных масок (от 1_{16} до 8_{16}).

Разработан и реализован алгоритм поиска максимальных вероятностей ЛК для масштабированных моделей различных БСШ с различным числом циклов.

Известны теоретические оценки ожидаемого значения максимальной вероятности ЛК для случайной подстановки (см. представленную в этом же журнале статью «Свойства таблиц линейной аппроксимации случайной подстановки»). Для случайной подстановки 16 в 16 битов математическое ожидание максимального значения в таблице линейной аппроксимации составляет около 620. Для итеративного шифра при достижении некоторого количества циклов этот параметр перестает изменяться. Поэтому в итоговой таблице 2 приведено минимальное количество циклов, при котором шифры достигают теоретически ожидаемого максимального значения в таблице линейной аппроксимации.

Таблица 2

Шифры (блок 16 битов)	Мин. число циклов для достижения теорет. ож. значения максим. вероятности лин. аппроксимации
SPN xor	4
SPN add	4
SPN add xor	4
FN xor	7
FN add	6
FN add xor	7

4. ЦИКЛИЧЕСКИЕ СВОЙСТВА ШИФРОВ

С групповыми (циклическими) свойствами шифрующих преобразований связано и одно из важных свойств блочного шифра, используемого в режиме счетчика или в режиме с обратной свя-

зью по выходу (OFB) – значение периода гаммы шифрующей, влияющего на выбор системных характеристик соответствующего профиля защиты информации.

Предлагается подход к анализу циклических свойств шифрующих преобразований, основанный на использовании предположения о принадлежности подстановок, порождаемых БСШ, к числу подстановок случайного типа. В литературе были найдены теоретические оценки показателей, характеризующих циклические свойства подстановок. В том числе, случайная подстановка 16 в 16 битов обладает следующими параметрами:

– математическое ожидание количества циклов: 12;

– максимальное количество циклов при рассмотрении 2^{16} случайных подстановок: 26.

Для каждого из рассматриваемых шифров экспериментальным путем было определено количество циклов преобразований, при котором формируемая шифром подстановка обладает свойствами случайной подстановки. Полученные результаты представлены в табл. 3.

Таблица 3

Шифры (блок 16 битов)	Мин. число циклов для достижения теорет. ож. значений циклических параметров
SPN xor	3
SPN add	3
SPN add xor	3
FN xor	7
FN add	5
FN add xor	5

Анализируя полученные результаты следует заметить, что использование модульного сложения в качестве операции введения секретности позволяет улучшить циклические свойства фейстель-подобных шифров, однако не влияет на свойства SPN шифров.

5. СТОЙКОСТЬ К ИНТЕРПОЛЯЦИОННОЙ АТАКЕ И АТАКЕ ЛИНЕЙНЫХ СУММ

В работе [7] предложен алгоритм, позволяющий оценить стойкость шифра к атаке линейных сумм и интерполяционной атаке. На практике этот алгоритм реализуем для случая, когда строящийся полином $f_k(x)$ связывает значения одного байта открытого текста с одним байтом шифртекста. Полином $f_k(x)$ имеет следующий вид:

$$f_k(x) = \sum_{i=1}^{2^8} a_i(k) b_i(x),$$

где $x \in GF(2^8)$ – байт открытого текста, $a_i(k) \in GF(2^8)$ – ключезависимые коэффициенты, $\{b_i(x)\}$ – множество линейно независимых полиномов с коэффициентами из $GF(2^8)$ (атака линейных сумм эквивалентна интерполяционной атаке, когда $b_i(x) = x^{i-1}$).

Атака линейных сумм эффективна, когда N, число неизвестных ключезависимых коэффициентов $a_i(k)$, меньше, чем 2^8.

Алгоритм для оценки количества ключезависимых коэффициентов N из [7] был реализован и с его помощью был произведен поиск количества ключезависимых коэффициентов в полиномах, связывающих байты открытого текста и байты криптограмм для SPN- и фейстель-подобных шифров с размером блока 128 битов (шифры имеют такую же структуру преобразований, как на рис.1 и 2, отличие в размерах блока (128 битов) и подключа (128 и 64 бита)). Результаты тестирования представлены в табл. 4.

Таблица 4

Шифры (блок 128 битов)	Мин. число циклов для обеспечения стойкости к интерполяционной атаке
SPN xor	3
SPN add	2
SPN add xor	2
FN xor	5
FN add	4
FN add xor	4

ВЫВОДЫ

Максимальные вероятности дифференциалов и линейных корпусов для SPN- и фейстель-подобных шифров не зависят от используемых операций введения секретности. Чередование нескольких операций сложения также не оказывает существенного влияния на значения указанных параметров.

Использование нескольких операций введения секретности позволяет улучшить циклические свойства и повысить стойкость шифра к алгебраическим атакам, таким как интерполяционная атака и атака линейных сумм. Но и в этом случае выигрыш составляет не более одного цикла преобразований как для SPN-, так и для фейстель-подобных шифров.

Литература:

[1] *J.L. Massey,* «SAFER K-64: A byte-oriented block-ciphering algorithm», R. Anderson, editor, Fast Software Encryption, Cambridge Security Workshop (LNCS 809), 1–17, SpringerVerlag, 1994.

[2] *Горбенко І.Д., Долгов В.І., Олійников Р.В., Руженцев В.І. та інші.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація» // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. Том. 6. № 2. – С. 195-208.

[3] *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника: научн.-техн. журнал. – 2007. Том. 6. № 2. – С. 230-240.

[4] *E. Kleiman.* The XL and XSL attacks on Baby Rijndael. Thesis, 2005, available from http://orion.math.iastate.edu/dept/thesisarchive/MS/EKleimanMSSS05.pdf.

[5] *Долгов В.И., Руженцев В.И.* «Сравнительный анализ криптостойкости уменьшенных моделей блочных шифров» // Праці міжнар. симпозіуму «Питання оптимізації обчислень» (ПОО), 24-29 вересня 2009. Київ: Інститут кібернетики ім. Глушкова НАН України, 2009. Т.1. С. 211-215.

[6] *Долгов В.И., Руженцев В.И., Олейников Р.В.* Дифференциальные свойства масштабированных моделей блочных симметричных шифров, 11-ая Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах», 20-23 мая 2008. Тезисы докладов. – К.: ЧП «ЕКМО» НИЦ «ТЕЗИС» НТУУ «КПИ», 2008.

[7] *K. Aoki.* Practical Evaluation of Security against Generalized Interpolation Attack. IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan), Vol. E83-A, No. 1, pp. 33–38, 2000. (A preliminary version was presented at SAC'99).

Поступила в редколлегию 9.07.2010.

Руженцев Виктор Игоревич, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, криптоанализ блочных симметричных шифров.

Ступак Валерий Владимирович, начальник отдела НКАУ, соискатель кафедры БИТ ХНУРЭ. Область научных интересов: криптография, системы защиты информации, криптоанализ блочних симметричных шифров.

УДК 621. 391:519.2:519.7

Криптографічна стійкість блокових шифрів при використанні різних операцій додавання з підключами / В.І. Руженцев, В.В. Ступак // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 361-364.

Досліджується кріптографічна стійкість блокових симетричних шифрів при використанні різних операцій додавання підключей. Досліджується стійкість до диференційних, лінійних, алгебраїчним та іншим атакам.

Ключові слова: блоковий симетричний шифр, криптографічна стійкість.

Табл. 4. Іл. 2. Бібліогр.: 7 назв.

UDC 621. 391:519.2:519.7

Cryptographic strength of block ciphers with using different sub-key addition operations / V.I. Ruzhentsev, V.V. Stupak // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 361-364.

The paper investigates the cryptographic strength of block symmetric ciphers with using different sub-key addition operations. The strength to differential, linear, algebraic and other attacks is considered.

Key words: symmetric block cipher, cryptographic strength.

Tab. 4. Fig. 2. Ref.: 7 items.