УДК 681.3.06: 519.248.681

В.И. РУЖЕНЦЕВ, канд. техн. наук, Р.В. ОЛЕЙНИКОВ, канд. техн. наук

ОСОБЕННОСТИ РЕАЛИЗАЦИИ НАИБОЛЕЕ ЭФФЕКТИВНЫХ КРИПТОАНАЛИТИЧЕСКИХ АТАК НА СТАНДАРТ ШИФРОВАНИЯ FIPS-197

Сегодня для Украины актуален вопрос принятия нового стандарта шифрования данных. В качестве одного из претендентов на национальный стандарт может рассматриваться новый американский стандарт блочного симметричного шифрования FIPS-197 [1] (AES – Advanced Encryption Standard). В этих условиях актуально исследование особенностей этого достаточно нового шифра, в частности анализ криптостойкости этого шифра, поскольку требование стойкости к криптоаналитическим атакам в настоящее время считается одним из основных для блочных симметричных шифров. В целях изучения известных результатов о стойкости этого шифра к различным методикам криптонападений было решено реализовать несколько наиболее эффективных методов криптоанализа на практике. На наш взгляд, только в этом случае можно считать, что та или иная методика криптоанализа достаточно глубоко изучена и освоена.

Целью данной работы – изложение основных результатов, полученных при реализации на практике интегральной (square) атаки и атаки невыполнимых дифференциалов на ослабленный алгоритм шифрования FIPS-197.

В спецификации шифра [2], а также некоторых других работах [3 – 5] представлены результаты оценки стойкости алгоритма шифрования к различным криптоаналитическим атакам. Эти результаты сведены в табл. 1.

Таблица 1

Виды криптоатак	Минимальное число циклов, при котором шифр стойкий	Показатели известных атак на AES (rijndael-128)		
		Максимальное число циклов	Вычислительные ресурсы, экв. опер.	Память
Дифференциальная	4	3	2^{54}	мало
Линейная	4			
Усеченный дифференциал	4	3	2^{8}	мало
Невозможный дифференциал	6	5	2^{36}	2^{42}
Интерполяционная	5			
Интегральная	7	6	2^{72}	2^{32}

Из представленных в таблице данных следует, что наиболее эффективными из известных криптоаналитических методик являются интегральная атака и атака невыполнимых дифференциалов. Обе эти атаки относятся к классу атак с подобранными открытыми текстами, то есть для их реализации криптоаналитику необходимо иметь достаточное множество криптограмм, полученных при зашифровании специально подобранных открытых текстов на одном и том же секретном ключе (см. рис. 1).

Интегральная атака на шифр rijndael (FIPS-197) предложена в [2]. Интегральной атака так названа, потому что в атаке рассматривается прохождение через преобразования шифра суммы состояний. Здесь и далее 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.

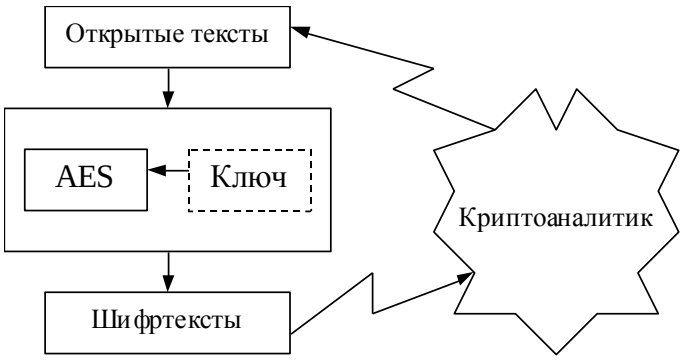

Рис. 1

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. Опираясь на известные источники [2, 3], изложим более подробно основные моменты организации атаки.

В атаке используется та особенность шифра, что при подаче на вход шифра множества специально подобранных открытых текстов сумма всех состояний, полученных при трехцикловом зашифровании, будет равняться 0 на всех битовых позициях. Последовательность изменения суммы состояний при выполнении трех циклов шифрующих преобразований представлена на рис. 2.

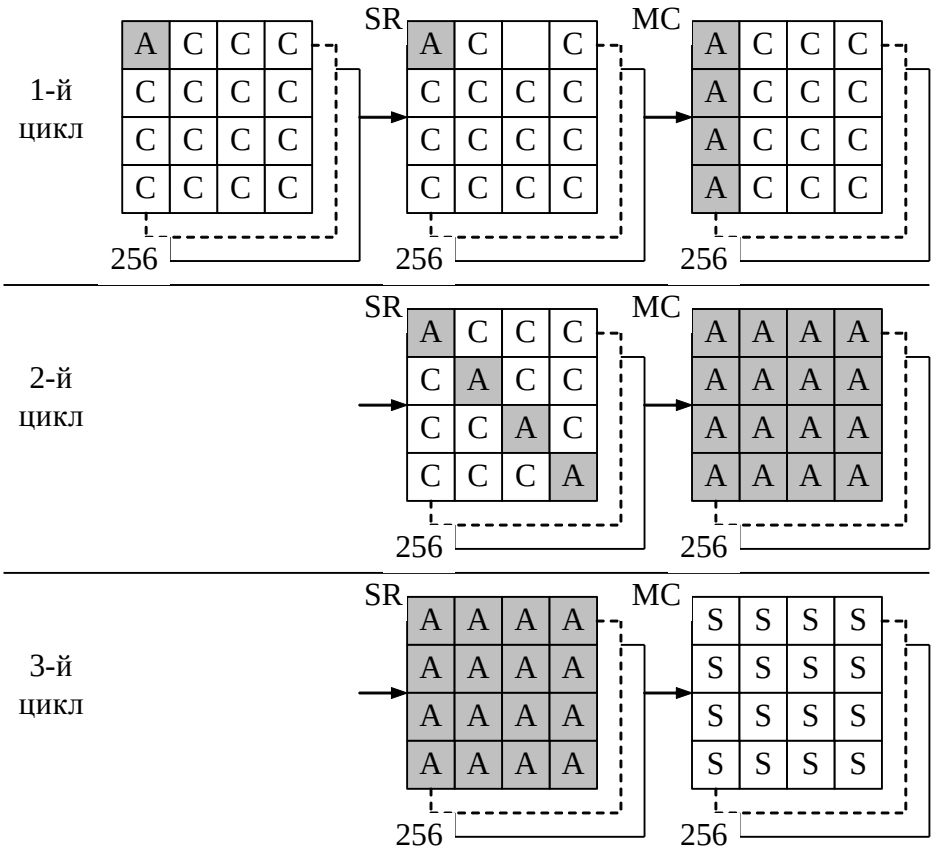

Рис. 2

Итак, на вход шифра (рис. 2) поступает множество из 256 открытых текстов, которое содержит один активный байт (обозначен буквой «A»), в котором каждый открытый текст содержит отличное от остальных открытых текстов значение, и 15 пассивных байтов, в которых все 256 состояния содержат одинаковые значения (обозначены символом «C»). Символом «S» отмечены байты, в которых при суммировании всех 256 состояний будет получен 0, при этом на позициях, отмеченных символами «A» и «C», также при суммировании будут получены 0.

Рассмотрим теперь прохождение исходного множества через преобразования шифра. Заметим, что операции нелинейной подстановки (*ByteSub*) и сложения с ключом (*AddRK*) не изменяют характер множества, которое состоит из байтов A и C. Поэтому на рис. 2 эти преобразования не отражены.

ShiftRow изменяет позиции активных байтов. Если на вход операции *MixColumn* поступает 4-байтовая колонка с одним активным байтом, то на выходе преобразования будет получено 4 активных байта [2, 3]. Действительно, рассмотрим две 4-байтовые колонки, которые отличаются в одном (первом) байте: (a’, b, c, d) и (a, b, c, d). Разность между этими колонками после их умножения на матрицу в ходе операции *MixColumn* будет равна (02·(a’⊕a), 01·(a’⊕a), 01·(a’⊕a), 03·(a’⊕a)). Поскольку в первом цикле на вход *MixColumn* поступают 256 состояний, любые два из которых отличаются в одном байте первой колонки и совпадают в остальных, то после этой операции любые два состояния из рассматриваемого множества будут отличаться в 4 байтах первой колонки. Следовательно, в каждом из 256 состояний в этих 4 байтах будут содержаться значения, отличающееся от значений на этих позициях в остальных 255 состояниях, другими словами эти четыре байта будут активными для рассматриваемого множества состояний, то есть будут обозначаться символом “A”.

Проследим теперь преобразование исходного множества открытых текстов при его прохождении через циклы алгоритма. До первой операции *MixColumn* характер множества не изменится. Операция *MixColumn* первого цикла преобразует множество с одним активным байтом в множество с четырьмя активными байтами. Эти четыре активных байта попадают по одному в разные 4-байтовые колонки в результате выполнения последующей операции *ShiftRow*, и поэтому после операции *MixColumn* второго цикла множество будет содержать 16 активных байтов (см. рис. 2).

До операции характер множества не изменится. Рассмотрим более детально операцию *MixColumn* третьего цикла. Если обозначить байты до этого преобразования через a, а после преобразования – b, то для каждого байта на выходе преобразования можно записать

$$\begin{aligned} \bigoplus_{256} b_{i,j} &= \bigoplus_{256} (2\cdot a_{i,j} \oplus 3\cdot a_{i+1,j} \oplus 1\cdot a_{i+2,j} \oplus 1\cdot a_{i+3,j}) = \\ &= 2\cdot(\bigoplus_{256} a_{i,j}) \oplus 3\cdot(\bigoplus_{256} a_{i+1,j}) \oplus (\bigoplus_{256} a_{i+2,j}) \oplus (\bigoplus_{256} a_{i+3,j}) \end{aligned} \qquad (1)$$

Поскольку до преобразования побитовая сумма по модулю 2 всех 256 состояний равнялась 0 на всех позициях, то равенство (1) приводится к соотношению

$$2\cdot 0 \oplus 3\cdot 0 \oplus 0 \oplus 0 = 0.$$

Это означает, что сумма всех состояний после операции *MixColumn* третьего цикла попрежнему будет давать 0 во всех битовых позициях (на рис. 2 байты состояний после этой операции обозначены «S»). Это свойство рассматриваемого множества нарушает операция *ByteSub* четвертого цикла, поэтому для шифра Rijndael удается провести сумму только через три цикла, но как показано в [2, 3], этого достаточно для организации атаки даже на шестицикловый шифр. Параметры известных интегральных атак на шифр AES сведены в табл. 3.

Из табл. 3 видно, что на практике достаточно просто может быть реализована атака на четырехцикловый шифр. Сценарий атаки состоит из следующих основных шагов:

1. Формируется 256*2 специальных открытых текстов и вырабатываются соответствующие им криптограммы.

2. Последовательно по очереди подбирается каждый байт подключа последнего (четвертого) цикла, таким образом, чтобы при дешифровании последнего цикла получилось множество состояний, сумма которых даст 0 в соответствующем байте состояния.

3. Из найденного на предыдущем этапе подключа четвертого цикла восстанавливается исходный секретный (мастер) ключ.

Таблица 3

Количество циклов	Требуемые ресурсы	
	Затраты на вычисления, операции шифрования	Память, байты
4	2^9	2^9
5	2^{40}	2^{11}
6	2^{72}	2^{32}

В соответствии с описанной методикой разработана программная реализация атаки на шифр rijndael с четырьмя циклами. Реализация выполнена в виде двух приложений. Первое приложение, используя ключ из файла 1, формирует необходимые пары открытый текст-криптограмма и сохраняет их в файлах. Второе приложение считывает криптограммы из соответствующего файла, используя криптограммы последовательно определяет все байты подключа четвертого цикла. Затем, из этого подключа восстанавливает исходный секретный ключ, который сохраняется в файле 2. В результате в файлах 1 и 2 оказываются идентичные ключи.

Основными итогами проведенного вычислительного эксперимента стало следующее:

- подтверждена правильность расчетов относительно возможности выполнения интегральной атаки и требуемых для этого вычислительных затрат и затрат памяти;
- продемонстрировано, что при возможности выбора около 512 открытых текстов и получении соответствующих им криптограмм секретный ключ, используемый в четырехцикловом шифре Rijndael, может быть определен со сложностью близкой к 2^9 операций шифрования, то есть такой ослабленный алгоритм взламывается в считанные доли секунды на любом компьютере.

Атака невыполнимых дифференциалов на шифр AES предложена в работе [3]. Данная криптоаналитическая методика называется атакой невыполнимых дифференциалов, поскольку в атаке используются дифференциалы специального вида – те, которые не могут выполниться, т. е. имеющие нулевую вероятность. Атака невыполнимых дифференциалов на r-цикловый шифр обычно становится возможной, когда имеется (r-1)-цикловый невыполнимый дифференциал.

Суть атаки заключается в следующем: на некотором цикле (обычно первом или последнем) делается предположение о примененном подключе или о его части (выполняется перебор цикловых ключей), а на остальных циклах предполагается выполнение “невыполнимого” дифференциала. Если на проверяемом цикловом ключе-кандидате возможно получение разностей, определенных “невыполнимым” дифференциалом, то этот ключ отбрасывается как ошибочный. В результате такого перебора остается ограниченное множество цикловых ключей-кандидатов.

Используя материалы работы [3], изложим более подробно основные моменты организации атаки невыполнимых дифференциалов на шифр Rijndael.

В основе известной атаки на пятицикловый шифр лежит четырехцикловый невыполнимый дифференциал, который используется для циклов со 2-го по 5-й (см. рис. 3).

На рис. 3 закрашенные ячейки обозначают наличие в соответствующем байте разности, отличной от нуля, незакрашенные ячейки обозначают нулевую разность

При прохождении разности через преобразования шифра позиции активных байтов изменяются при выполнении преобразований *ShiftRow* и *MixColumn* (на рис. 3 обозначается как SR и MC).

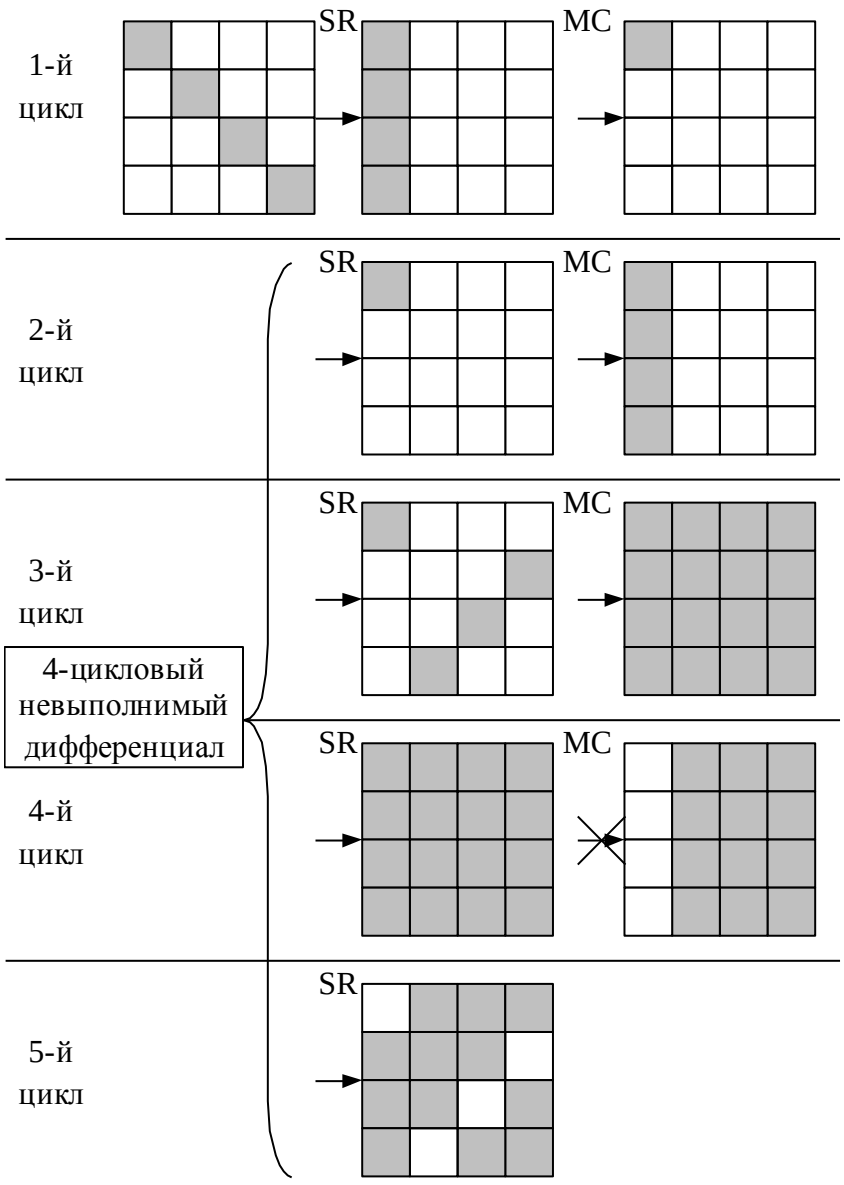

Рис. 3

Если *ShiftRow* просто меняет позиции активных байтов, то *MixColumn* меняет как позиции, так и количество активных байтов в рамках каждой колонки таким образом, что суммарное число активных байтов до и после этого преобразования в любой колонке не менее 5 (кроме случая, когда разность на входе в преобразование не содержит ни одного активного байта в колонке – тогда выходная разность также не будет содержать активных байтов). Случай, когда на вход операции *MixColumn* поступает четырехбайтовая колонка с одним активным байтом, рассмотрен при описании интегральной атаки, и как уже было показано, в этом случае на выходе преобразования всегда будет получаться четыре активных байта.

В соответствии с приведенным на рис. 3 четырехцикловым невыполнимым дифференциалом, если на входе имеется разность в одном байте (любом из четырех), то после четырех циклов не может быть получена разность с нулевыми значениями хотя бы в одной из комбинаций байтов 0,7,10,13; 1,4,11,14; 2,5,8,15; 3,6,9,12 (каждая комбинация соответствует одной пассивной колонке после операции *MixColumn* четвертого цикла). В ходе выполнения атаки рассматриваются пары открытых текстов, которые обладают заданным входным значением разности (начальное значение на рис. 3). Эти пары зашифровываются пятицикловым алгоритмом. Если разность какой-либо пары криптограмм оказывается равной нулю в одной из

перечисленных комбинаций байтов, то это значит, что после первого цикла не могла быть получена разность с единственным активным байтом, и поэтому подключи первого цикла, которые позволяют получить один активный байт после первого цикла, являются неверными. Эти варианты ключей находятся традиционным для дифференциального криптоанализа путем, рассматриваются последовательно все возможные варианты разности на выходе первого цикла, в которых активен один байт.

В ходе исследований нами была предложена атака на четырехцикловый шифр, которая требует значительно меньших вычислительных затрат и затрат памяти и поэтому может быть реализована на практике. Показатели известной и предлагаемой атак представлены в табл. 4.

Таблица 4

Количество циклов	Требуемые ресурсы		
	Затраты на вычисления, операции шифрования	Память, байты	Количество пар открытых текстов-криптограмм
4	2^{33}	2^{29}	2^{16}
5	2^{36}	2^{42}	$2^{29,5}$

Схема предлагаемой атаки представлена на рис. 4.

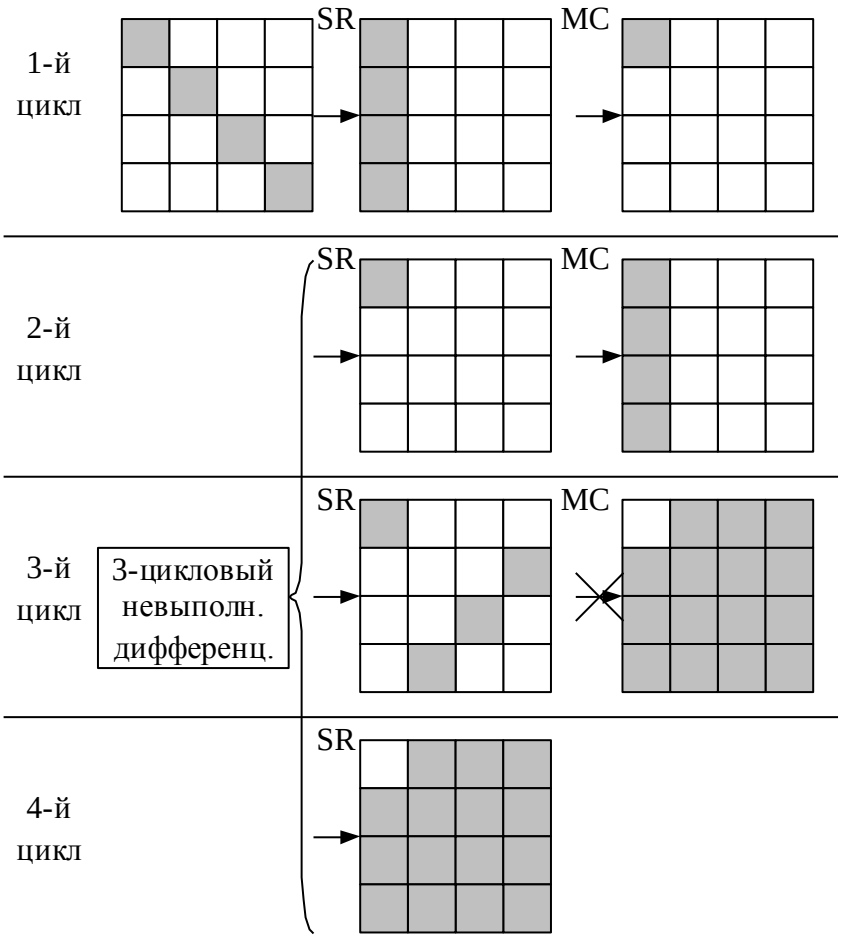

Рис. 4

В предлагаемой атаке используется трехцикловый невозможный дифференциал, который представлен на рис. 4. Если на вход второго цикла поступает разность с одним активным байтом (этот байт может находиться на любой позиции), то после четвертого цикла все байты должны быть активными, т.е. должны содержать ненулевую разность, следовательно, выходная разность хотя бы с одним пассивным байтом получиться не может.

В ходе атаки рассматриваются пары открытых текстов, обладающие заданной входной разностью (активные байты расположены по главной диагонали (см. рис. 4)). Для этих открытых текстов вырабатываются криптограммы с использованием четырехциклового алгоритма шифрования. И если разность криптограмм равна нулю хотя бы в одном из байтов, то это свидетельствует о том, что на входе второго цикла не могла быть разность с только одним активным байтом. Поэтому все подключи первого цикла, которые приводят к такой ситуации, следует отбросить как неверные. Целью атаки является нахождение и исключение всех неверных ключей, в результате должен остаться только один вариант 32-битного фрагмента подключа первого цикла, который и будет верным.

Выполненные расчеты показали, что для исключения всех неправильных 32-битных фрагментов ключа необходимо проанализировать около 2^{16} открытых текстов, из которых может быть составлено примерно $(2^{16})^2/2 = 2^{31}$ пар с нужной входной разностью и найдено около $\frac{2^{31}}{16} = 2^{27}$ пар, которые обладают при этом и требуемой выходной разностью. Таким образом, сценарий предлагаемой атаки состоит из следующих этапов:

1. Формируется 2^{16} специфических открытых текстов и с помощью четырехциклового алгоритма вырабатываются соответствующие им криптограммы.

2. Среди криптограмм находятся такие пары, разность которых равна 0 хотя бы в одном байте.

3. Последовательно рассматриваются 2^{10} варианта разности с одним активным байтом на выходе первого цикла, для каждого варианта находятся ключи, которые для данных открытых текстов позволяют получить такую разность после первого цикла. Все найденные на третьем шаге 32-битные фрагменты подключа первого цикла исключаются из полного множества 2^{32} вариантов.

В результате атаки необходимо исключить все неправильные 32-битные фрагменты подключа первого цикла.

В соответствии с описанной методикой разработана программная реализация атаки на шифр Rijndael с четырьмя циклами. Атака реализована в виде двух приложений. Первое приложение, используя 16-байтовый ключ из файла, позволяет набрать необходимое количество пар открытый текст-криптограмма и сохранить их в файлах. Второе приложение считывает открытые тексты и криптограммы из соответствующих файлов и, действуя дальше по изложенной методике, начинает находить неверные варианты 32-битного фрагмента подключа первого цикла. Каждый найденный неверный вариант фрагмента фиксируется единичным значением в бите, который соответствует этому значению в массиве из 2^{32} битов. С определенным интервалом массив из 2^{32} битов (2^{29} байтов) сохраняется в файле.

В ходе вычислительного эксперимента приложение, которое определяет неверные 32-битные фрагменты подключа первого цикла, проработало около 20 часов и за это время обнаружило около 30 000 000 $\approx 2^{24,8}$ неверных вариантов 32-битного фрагмента, проанализировав при этом $\approx$ 29000 пар открытых текстов, которые обладают требуемой входной разностью и чьи криптограммы содержат нулевую разность хотя бы в одном байте. От общего числа таких пар, которое необходимо рассмотреть, это составляет $\frac{29000}{2^{27}} \cdot 100\,\% = 0{,}02\,\%$. Исходя из этого для завершения работы потребуется 5000*20 = 100000 часов.

Вычислительный эксперимент показал, что методика невыполнимых дифференциалов является достаточно ресурсоемкой, поскольку в отличие от криптоаналитических атак, в которых выполняется поиск верных значений ключа, здесь верное значение находится путем исключения всех неверных значений из достаточно большого числа вариантов. Поэтому даже для шифра с небольшим количеством циклов, реализация атаки невыполнимых дифференциалов сопряжена с относительно высокими вычислительными затратами и затратами памяти.

В ходе выполненного вычислительного эксперимента было выявлено значительное расхождение между теоретическими и практическими показателями сложности данной атаки. На наш взгляд, в первую очередь, это можно объяснить тем, что теоретический расчет сложности атаки не учитывает высокой ресурсоемкости работы с массивами большой размерности.

При этом результаты вычислительного эксперимента подтвердили работоспособность данной криптоаналитической методики, которая для многих шифров, в том числе и для четырех- или пятициклового алгоритма AES, является одной из наиболее эффективных.

Следует отметить, что реализация атаки невыполнимых дифференциалов без особых трудностей может быть распараллелена для решения на нескольких ЭВМ, что позволит снизить временные затраты на реализацию данной атаки в соответствующее число раз.

Список литературы: 1. *National* Institute of Standards and Technology Advanced encryption algorithm (AES) development // FIPS 197, U.S. Department of Commerce, Nov. 2001. 2. *Daemen, J., Rijmen, V.* AES Proposal Rijndael, AES Round 1 Technical Evaluation CD-1: Documentation, National Institute of Standards and Technology, Aug 1998. See http://www.nist.gov/aes. 3. *Biham, E., Keller, N.* Cryptanalysis of Reduced Variant of Rijndael, http://cscr.nist.gov/encryption/aes/round2/conf3/aes3papers.html. 4. *Sugita, M., Kobara, K.* Relationships among differential, truncated differential, impossible differential cryptanalyses against word-oriented block cipher like Rijndael, E2 // National Institute of Standards and Technology, http://www.nist.gov/aes. 5. *Aoki, K.* 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).

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 10.05.2012