УДК 681.3.06: 519.248.681

В.И. РУЖЕНЦЕВ

Харьковский национальный университет радиоэлектроники, Украина

ДОКАЗУЕМАЯ СТОЙКОСТЬ RIJNDAEL-ПОДОБНЫХ ШИФРОВ К АТАКЕ УСЕЧЕННЫХ ДИФФЕРЕНЦИАЛОВ

Рассматривается стойкость rijndael-подобных алгоритмов шифрования к атаке усеченных дифференциалов. Доказываются теоремы об отсутствии эффективных байтовых дифференциальных характеристик и эффективных байтовых дифференциалов для шифров с достаточным числом циклов, что свидетельствует о защищенности от атаки усеченных дифференциалов. Основной итог работы заключается в том, что удалось доказать отсутствие эффективных байтовых дифференциалов для определенного числа циклов Rijndael-подобных шифров, значит эти шифры можно считать доказуемо стойкими к атаке усеченных дифференциалов.

Ключевые слова: *блочный симметричный шифр, криптоаналитическая атака, дифференциальная характеристика, дифференциал, усеченный (байтовый) дифференциал.*

Введение

Шифр Rijndael – один из наиболее распространенных алгоритмов шифрования и средство обеспечения конфиденциальности в мире, поэтому вопросы анализа его криптоаналитической безопасности являются актуальными. В ряде наших предыдущих работ [1 – 3] изучалась стойкость алгоритма к атаке усеченных дифференциалов и в [3] нам удалось обосновать отсутствие эффективных байтовых дифференциальных характеристик (БХ) для 3 и более циклов 128-битного варианта шифра Rijndael. Однако для обоснования доказуемой стойкости необходимо также доказательство отсутствия эффективных байтовых дифференциалов (БД), что и является целью настоящей работы.

Работа построена следующим образом. Сначала мы напомним базовые понятия, связанные с атакой усеченных дифференциалов, затем, предложим альтернативный вариант доказательства теоремы из [3] об отсутствии эффективных БХ для шифра Rijndael и, наконец, докажем ряд лемм и утверждений, которые позволят доказать основную теорему об отсутствии эффективных БД.

1. Атака усеченных дифференциалов

Методика реализации атаки усеченных дифференциалов была предложена Л. Кнудсеном [4]. Отличие от обычной дифференциальной атаки заключается в том, что через циклы проводится не полная разность, а некоторая ее часть. В работе [4] показано, что такая методика эффективна в случаях, когда в шифре используется недостаточно хорошее рассеивание и прохождение разности через несколько циклов может рассматриваться независимо от значения разности в некоторой части блока.

Один из вариантов атаки – атака байтовых дифференциалов – была предложена в работах [5,6]. В ходе атаки через преобразования шифра пытаются провести вектора активизации. Каждый бит вектора активизации отражает активность одного байта в обычной разности. Таким образом, вектор активизации содержит столько битов, сколько байтов в блоке, а значение бита определяется активностью байта: «1» - байт активный, «0» – байт пассивный.

Совокупность значений входного и выходного векторов активизации для одного цикла преобразований называется *одноцикловой байтовой характеристикой*. По аналогии с обычным дифференциальным криптоанализом «сшивку» нескольких одноцикловых БХ (условие «сшивки»: входной вектор активизации каждой последующей одноцикловой БХ равен выходному вектору активизации предыдущей) будем называть *многоцикловой БХ*. Вероятность такой характеристики вычисляется как произведение вероятностей всех входящих в нее одноцикловых характеристик. БХ, покрывающие одинаковое число циклов и имеющие одинаковые значения входных векторов активизации и одинаковые значения выходных векторов активизации, принадлежат одному и тому же *байтовому дифференциалу*. Вероятность БД есть сумма вероятностей всех входящих в него БХ.

Напомним также, что БХ или БД считаются *эффективными*, когда их вероятность $p_{бх}$ или $P_{бд}$ больше вероятности получения на выходе того же вектора активизации при произвольном (случайном)

векторе активизации на входе (случайный входной вектор активизации предполагает равновероятность всех значений выходной разности):

$$P_{бд} > p_{сл} \text{ или } p_{бх} > p_{сл}, \quad (1)$$

где $p_{сл} \approx \left(2^{-8}\right)^{u}$, u – число неактивных байтов в выходной разности или число нулевых битов в выходном векторе активизации. Следует заметить, что для эффективного БД или БХ непременно будет выполняться и традиционное для обычных дифференциалов ограничение: $P_{бд} > 2^{-n}$ или $p_{бх} > 2^{-n}$), где n – длина блока в битах.

Если удается найти эффективный дифференциал, то обычно на последнем цикле, где известны выходное значение разности (на основе известных значений криптограмм) и входной вектор активизации (в соответствии с используемым байтовым дифференциалом). Эта информация позволяет получить информацию о подключе последнего цикла. Таким образом, для выполнения атаки необходимо, чтобы БД или БХ покрывали все циклы шифра.

2. Обоснование отсутствия эффективных байтовых дифференциальных характеристик для Rijndael-подобных шифров

В настоящей работе будет обсуждаться стойкость Rijndael-подобных шифров, то есть алгоритмов шифрования, которые содержат в каждом цикле (даже в последнем) четыре вида преобразований - аналоги преобразований шифра Rijndael: ByteSub, ShiftRow, MixColumns и AddKey. В зависимости от размера блока может меняться количество колонок.

Прежде чем перейти к рассмотрению стойкости Rijndael к атаке рассмотрим особенности преобразования MixColumns, так как именно это преобразование вносит неопределенность в прохождение векторов активизации через циклы шифра. В работе [2] проведен анализ этого преобразования и определены вероятности переходов векторов активизации через MixColumns. В табл. 1 представлены двоичные логарифмы от вероятностей перехода векторов активизации через MixColumns для различного числа активных битов на входе (меняется по столбцам) и выходе (по строкам).

Теперь перейдем к доказательству теоремы из [3] об отсутствии эффективных БХ. Сначала покажем справедливость леммы.

Лемма 1. Для Rijndael-подобного шифра с k колонками в блоке нет эффективных байтовых дифференциальных характеристик с k или более активными колонками на входе преобразований MixColumns.

Таблица 1

Log_2 вероятности перехода вектора активизации через MixColumns

Вход / Выход	0	1	2	3	4
0	0	-	-	-	-
1	-	-	-	-	0
2	-	-	-	-7,99	-0,023
3	-	-	-15,99	-8,017	-0,0226
4	-	-23,983	-16,0115	-8,0171	-0,0226

Доказательство. В соответствии с табл. 1, для преобразования MixColumns за каждый дополнительный пассивный байт на выходе вероятность уменьшается примерно в 28 раз. Таким образом, если в байтовой характеристике встречается k активных колонок, то на выходе будут либо все активные байты, либо за каждый пассивный байт вероятность характеристики уменьшится в 28 раз. То есть, в лучшем случае, итоговая вероятность будет приблизительно равна pcл, а значит не будет эффективной. Лемма доказана.

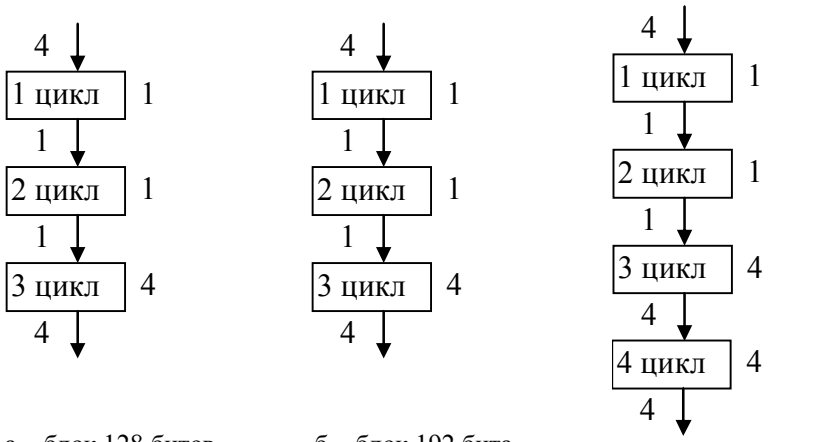
Теперь, используя доказанную в [7] лемму о минимальном количестве активных колонок на входе и выходе двух последовательных циклов (минимальное количество таких колонок – 5), представим альтернативный вариант доказательства теоремы об отсутствии эффективных БХ, который на наш взгляд, является более наглядным и простым, чем вариант из [3].

Теорема 1 ([3]). Для шифра Rijndael с размером блока 128, 192 и 256 битов нет эффективных БХ, соответственно, для 3, 3 и 4 или более циклов с полным набором преобразований.

Доказательство. Для доказательства теоремы необходимо оценить минимальное количество активных колонок для каждого из вариантов шифра.

На рис. 1 представлены, на наш взгляд, варианты с минимальным количеством активных колонок на входах в преобразования MixColumns для 3-х вариантов размера блока. На рис. 1 справа от каждого цикла указано количество активных колонок на входе в преобразование MixColumns и оно всегда совпадает с количеством активных колонок на выходе цикла. Сверху и снизу от каждого цикла на рис. 1 указано количество активных колонок до и после цикла и оно выбирается в соответствии с условиями леммы из [7], но при этом не может быть меньше 1.

В соответствии с леммой из [7], вход и выход 2-го и 3-го цикла содержит не менее 5 активных колонок. Соответственно, не менее 5 активных колонок будет содержаться на входе преобразований MixColumns в 1-м и 3-м циклах.



а – блок 128 битов б – блок 192 бита в – блок 256 битов

Рис. 1. Количество активных колонок

Плюс к этому минимум одна активная колонка во 2-м цикле. Таким образом, для 3-х циклов Rijndael минимальное количество активных колонок на входе преобразований MixColumns – 6. Тогда, в соответствии с леммой 1, для 3-х циклов Rijndael-128 нет эффективных БХ.

Для размера блока 192 бита ситуация аналогична (см. рис. 1, б): 3 цикла гарантируют минимум 6 активных колонок на входах преобразований MixColumns – следовательно, в соответствии с леммой 1, отсутствуют эффективные БХ.

Для размера блока 256 бита 3 цикла также гарантируют минимум 6 активных колонок на входах преобразований MixColumns, но этого мало для применения леммы 1, так как общее число колонок в блоке – 8. Поэтому необходим четвертый цикл. Для четырех циклов минимальное количество активных колонок на входах преобразований MixColumns составляет 10 (см. рис. 1,в), а значит нет эффективных БХ для размера блока 256 битов при 4 и более циклах. Теорема доказана.

3. Обоснование отсутствия эффективных байтовых дифференциалов для Rijndael-подобных шифров

Теперь перейдем к рассмотрению байтовых дифференциалов. Начнем с рассмотрения шифра со 128-битовым блоком. Справедливо следующее утверждение.

Утверждение 1. Для каждого не невыполнимого r-циклового ($r \geq 3$) БД всегда есть одна и только одна БХ с вероятностью примерно $p_{сл}*2^{-0,0904*r}$.

Доказательство. Известно несколько невыполнимых БД, которые лежат в основе атаки невыполнимых дифференциалов. Для всех остальных БД существует БХ, в которой на выходе всех преобразований MixColumns кроме последнего и предпоследнего циклов будет формироваться вектор активизации со всеми активными байтами. В большинстве случаев (см. 4-ю колонку табл. 1) вероятность такого перехода для одной колонки составит $2^{-0,0226}$. Если активны все 4 колонки, а такая ситуация в данном случае возникнет максимум после одного цикла, то вероятность будет уменьшаться в $2^{-0,0226*4} = 2^{-0,0904}$ раз на каждом цикле. В итоге, за каждый пассивный байт в выходной разности в последнем и, в некоторых случаях, предпоследнем циклах заплатим уменьшением вероятности в 2^8 раз. Кроме того, каждый дополнительный цикл будет уменьшать вероятность примерно в $2^{-0,0904}$ раз. Таким образом, итоговая вероятность такой БХ составит $p_{сл}*2^{-0,0904*r}$.

В дальнейшем подобную БХ будем называть *основной*, а остальные БХ, принадлежащие этому же БД, будем называть *дополнительными*.

Утверждение 2. Для каждого БД с 3 или более циклами любая дополнительная БХ с m дополнительными пассивными байтами имеет вероятность примерно в 2^{8m} раз ниже, чем основная БХ этого БД.

Доказательство. Каждая дополнительная БХ должна отличаться от основной и это отличие должно заключаться в одном или нескольких дополнительных пассивных байтах. При чем, дополнительные пассивные байты должны быть в тех циклах, где в основной БХ используются переходы с вероятностью около 1.

Таким образом, в соответствии с табл. 1 каждый дополнительный пассивный байт будет уменьшать вероятность БХ примерно в 2^8 раз. В итоге, вероятность БХ будет всегда примерно в 2^{8m} раз ниже, чем основная БХ этого БД.

Теорема 2. Для вариантов шифра Rijndael с размером блока 128, 192 и 256 битов нет эффективных БД, соответственно, для 3, 3 и 4 или более циклов.

Доказательство. Сначала рассмотрим Rijndael с блоком 128 и оценим количество дополнительных

БХ с различным количеством циклов и дополнительных пассивных байтов.

Итак, рассмотрим ситуацию с одним дополнительным пассивным байтом. Количество дополнительных БХ будет $C_R^1 \cdot C_{16}^1 = 16 \cdot R$, где первый множитель C_R^1 - это количество вариантов выбора цикла с этим пассивным байтом, а C_{16}^1 - количество вариантов расположения этого пассивного байта в блоке шифра. Таким образом, в соответствии с утверждением 2, суммарная вероятность БХ с одним дополнительным пассивным байтом составит $16R \cdot 2^{-8}$.

Есть три варианта расположения двух дополнительных пассивных байтов:

- одна колонка – количество вариантов $C_R^1 \cdot C_4^1 \cdot C_4^2 = R \cdot 4 \cdot 6 = 24 \cdot R$;

- один цикл, но разные колонки – количество вариантов $C_R^1 \cdot C_4^2 \cdot \left(C_4^1\right)^2 = 96 \cdot R$;

- два разных цикла – количество вариантов $C_R^2 \cdot \left(C_{16}^1\right)^2 = \frac{R!}{(R-2)! \cdot 2!} \cdot 256 = 128 \cdot R^2 - 128 \cdot R$.

Просуммировав эти значения, можем получить суммарную вероятность от БХ с двумя дополнительными пассивными байтами: $(128R^2 - 8R) \cdot 2^{-16}$.

Действуя аналогичным образом, мы оценили количество вариантов для дополнительных БХ с тремя дополнительными пассивными байтами. В этом случае количество вариантов расположения этих байтов значительно больше и составляет, в итоге, $683R^3 - 128R^2 + 5R$. Как и в случае с двумя байтами, в итоговом значении можно выделить наиболее весомое слагаемое $683R^3$. Можно пренебречь остальными слагаемыми и считать, что суммарная вероятность от БХ с тремя дополнительными пассивными байтами: $\approx 683R^3 \cdot 2^{-24}$.

Считая, что суммарная вероятность от БХ с i дополнительными пассивными байтами будет представлена только одним самым весомым элементом, и этот элемент присутствует когда $i \le R$, можно записать общую формулу для суммарной вероятности от БХ с i дополнительными пассивными байтами:

$$\frac{R^i \cdot 16^i \cdot 2^{-8i}}{i!} = \frac{\left(\frac{R}{16}\right)^i}{i!}$$

для i = 0, …, R (случай i = 0 соответствует основной БХ).

Для оценки вероятности БД, которая состоит из суммы вероятностей всех БХ принадлежащих БД, необходимо оценить сумму ряда:

$$\sum_{i=0}^{R} \frac{\left(\frac{R}{16}\right)^i}{i!}.$$

Из теории известно, что

$$\sum_{i=0}^{\infty} \frac{x^i}{i!} = e^x.$$

Тогда, в нашем случае:

$$\sum_{i=0}^{R} \frac{\left(\frac{R}{16}\right)^i}{i!} < \sum_{i=0}^{\infty} \frac{\left(\frac{R}{16}\right)^i}{i!} \approx e^{\frac{R}{16}}.$$

Теперь, используя утверждение 1, можно оценить вероятность БД с числом циклов, при котором отсутствуют эффективные БХ:

$$P_{БД} = e^{\frac{R}{16}} \cdot 2^{-0,0904 \cdot R} \cdot p_{сл} =$$

$$= \left(e^{\frac{1}{16}} \cdot 2^{-0,0904} \right)^R \cdot p_{сл} \approx$$

$$\approx 1^R \cdot p_{сл} = p_{сл}.$$

Таким образом, вероятность любого БД будет примерно равна $p_{сл}$, а такой БД не будет эффективным. Теорема доказана.

Выводы

Основной итог работы заключается в том, что нам удалось доказать отсутствие эффективных байтовых дифференциалов для определенного числа циклов Rijndael-подобных шифров. А значит эти шифры можно считать доказуемо стойкими к атаке усеченных дифференциалов.

Литература

1. Долгов, В.И. О методе выполнения оценки стойкости шифра Rijndael к дифференциальным атакам [Текст] / В.И. Долгов, В.И. Руженцев // Радиоэлектроника и информатика. – 2002. – № 1. – С. 136 – 138.

2. Руженцев, В.И. О методах оценки стойкости к атаке усеченных дифференциалов [Text] / В.И. Руженцев // Радиоэлектроника и информатика. – 2003. – No. 4. – P. 130 – 133.

3. Руженцев, В.И. Обоснование стойкости стандарта шифрования FIPS-197 к атаке усеченных дифференциалов [Текст] / В.И. Руженцев, Р.В. Олейников // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – 2008. – Т.7, № 3. – С. 225 – 227.

4. Knudsen, L.R. Truncated and Higher Order Differentials [Text] / L.R. Knudsen // B. Preneel, editor, Fast Software Encryption. — Second International Workshop, Volume 1008 of Lecture Notes in Computer

Science Springer-Verlag, Berlin, Heidelberg, New York, 1995. – P. 196 – 211.

5. Knudsen, L.R. Truncated differentials of SAFER [Text] / L.R. Knudsen, T.A. Berson. – In Fast Software Encryption - Third International Workshop, FSE'96, Volume 1039 of Lecture Notes in Computer Science, Berlin, Heidelberg, New York, Springer-Verlag. – 1996.

6. Matsui, M. Cryptanalysis of reduced version of the block cipher E2 [Text] / M. Matsui, T. Tokita // In pre-proceedings of Fast Software Encryption'99. – 1999. – P. 70 – 79.

7. AES Proposal Rijndael [Electronic resource] / J. Daemen, V. Rijmen. – Access mode: AES Round 1 Technical Evaluation CD-1: Documen-tation, National Institute of Standards and Technology, Aug 1998. See http://www.nist.gov/aes. – Aug. 1998.

Поступила в редакцию 12.03.2012

Рецензент: д-р техн. наук, проф., проф. кафедры БИТ В.И. Долгов**,** Харьковский национальный университет радиоэлектроники, Харьков, Украина.

ДОКАЗУЄМА СТІЙКІСТЬ RIJNDAEL-ПОДІБНИХ ШИФРІВ ДО АТАКИ УСІЧЕНИХ ДИФЕРЕНЦІАЛІВ

В.І. Руженцев

Розглядається стійкість rijndael-подібних алгоритмів шифрування до атаки усічених (байтових) диференціалів. Доводяться теореми про відсутність ефективних байтових диференційних характеристик та ефективних байтових диференціалів для шифрів з достатньою кількістю циклів, що свідчить про захищеність до атаки усічених диференціалів. Основний підсумок роботи полягає в тому, що вдалося довести відсутність ефективних байтових диференціалів для певного числа циклів Rijndael-подібних шифрів, означає, що ці шифри можна вважати доказово стійкими до атаки усічених диференціалів.

Ключові слова: блоковий симетричний шифр, криптоаналітична атака, диференціальна характеристика, диференціал, усічений (байтовий) диференціал.

PROVABLE SECURITY OF RIJNDAEL-LIKE CIPHERS TO TRUNCATED DIFFERENTIALS ATTACK

V.I. Ruzhentsev

The resistance of rijndael-like ciphers to the truncated differential attack is considered. The theorems about the absence of effective byte differential characteristics and effective byte differentials for ciphers with sufficient number of rounds are proved. It means that such ciphers are secure against this type of attack. Basic balance of the work consists in that it was succeeded to prove absence of effective byte differentials for the certain number of cycles of rijndael codes, means these codes it is possible to consider demonstrable proof to the attack of the truncated differentials.

Key words: block symmetric cipher, cryptanalytic attack, differential characteristic, differential, byte (truncated) differential.

Руженцев Виктор Игоревич – канд. техн. наук, доцент, доцент кафедры безопасности информационных технологий Харьковского Национального университета радиоэлектроники, Харьков, Украина, e-mail: vityazik@rambler.ru.