УДК 681.3.06: 519.248.681

ОБОСНОВАНИЕ СТОЙКОСТИ СТАНДАРТА ШИФРОВАНИЯ FIPS-197 К АТАКЕ УСЕЧЕННЫХ ДИФФЕРЕНЦИАЛОВ

В.И. РУЖЕНЦЕВ, Р.В. ОЛЕЙНИКОВ

Исследуется возможность построения эффективных байтовых усеченных дифференциалов для блочного симметричного шифра Rijndael, которые могут быть положены в основу атаки усеченных дифференциалов. Приводится теоретическое обоснование отсутствия таких дифференциалов для шифра с 3 и большим количеством циклов.

The opportunity of constructing effective truncated byte differentials for the block symmetric cipher Rijndael is investigated. The theoretical substantiation of absence of such differentials for the cipher with 3 and more rounds is provided.

Вопросы криптостойкости нового американского стандарта шифрования FIPS-197 [1] (AES или rijndael [2]) вызывают интерес у многих криптографов. Целью этой работы является обоснование стойкости этого алгоритма блочного симметричного шифрования к атаке усеченных (байтовых) дифференциалов.

Методика реализации атаки усеченных дифференциалов была предложена Л. Кнудсеном [3]. Отличие от обычной дифференциальной атаки заключается в том, что через циклы проводится не полная разность, а некоторая ее часть. В работе [3] 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.

Для байт-ориентированных шифров естественным считается изучение усеченных дифференциалов особого вида, для которых усечение заключается не в исключении из рассмотрения отдельных битов входной или выходной разности, а в рассмотрении активности s-блоков. поскольку используемые в современных шифрах s-блоки (s-подстановки) чаще всего являются отображениями байт-в-байт, то дифференциалы, характеризующие активность s-блоков, часто называют байтовыми дифференциалами. в байтовых дифференциалах разность представляется в виде последовательности битов, каждый из которых отражает активность одного s-блока (байта) (1 – ненулевая разность – s-блок активный; 0 – s-блок неактивный). то есть, при рассмотрении байтовых дифференциалов (бд) в определенном смысле происходит объединение некоторого множества дифференциальных характеристик, поэтому распространено мнение [4], что оценка вероятностей бд для байт-ориентированных шифров позволяет получить более точную оценку стойкости к дифференциальному криптоанализу (дк), чем при стандартном подходе, т.е. при рассмотрении максимальной вероятности отдельных дифференциальных характеристик.

В литературе существует описание атак усеченных (байтовых) дифференциалов на ослабленные варианты байт-ориентированных шифров safer и e2 [5,6].

Основываясь на [6-8], изложим основные понятия, связанные с усеченными (байтовыми) дифференциалами, важными понятиями при изучении байтовых дифференциалов являются функция или вес хэмминга (*h*-функция) и функция-характеристика (χ-функция). Вес хэмминга битовой последовательности равен числу ненулевых битов в этой последовательности. χ-функция задает отображение $\{0,1\}^n$ в $\{0,1\}$ следующим образом

$$\chi(a)=\begin{cases}0, \text{ если } a=0,\\ 1, \text{ если } a\neq 0,\end{cases}$$

где $a\in\{0,1\}^n$.

Если $x\in\{0,1\}^{nm}$, то $\chi(x)=\chi(x_0, x_1, ..., x_m)=(\chi(x_0), \chi(x_1), ..., \chi(x_m))$.

Если обозначить разность на входе и выходе циклового преобразования, включающего в себя m n-битных s-блоков, как $\Delta x=(\Delta x_0,\Delta x_1,...,\Delta x_m)$ и $\Delta y=(\Delta y_0,\Delta y_1,...,\Delta y_m)$ соответственно, то вектора активизации байтов $\delta x,\delta y\in\{0,1\}^m$ определяются как

$$\delta x=(\delta x_0,\delta x_1,...,\delta x_m), \text{ где } \delta x_i=\chi(\Delta x_i)\in\{0,1\},$$

$$\delta y=(\delta y_0,\delta y_1,...,\delta y_m), \text{ где } \delta y_i=\chi(\Delta y_i)\in\{0,1\}$$

вероятность перехода $\delta x\to\delta y$ в ходе циклового преобразования f для любых $\delta x,\delta y\in\{0,1\}^m$ и $\Delta x,\Delta y\in\{0,1\}^{nm}$ определяется следующим образом

$$p^{(1)}_{\text{бд}}(\delta x,\delta y)=\frac{\sum\limits_{\substack{\chi(\Delta x)=\delta x\\ \chi(\Delta y)=\delta y}}\Pr\left[F(x)\oplus F(x+\Delta x)=\Delta y\right]}{\#\{\Delta x\in\{0,1\}^{nm}\mid\chi(\Delta x)=\delta x\}}.$$

Совокупность значений входного и выходного векторов активизации для одного цикла преобразований называется одноцикловой байтовой характеристикой. Такая связь характеризуется вероятностью, которую будем обозначать как $p^{(1)}_{\text{бд}}(\delta x,\delta y)$, где δx и δy – входной и выходной вектора активизации. По аналогии с обычным дифференциальным криптоанализом «сшивку» нескольких одноцикловых байтовых характеристик (условие «сшивки»: входной вектор активизации каждой последующей одноцикловой байтовой ха-

рактеристики равен выходному вектору активизации предыдущей) будем называть *многоцикловой байтовой характеристикой*. Вероятность такой характеристики вычисляется как произведение вероятностей всех входящих в нее одноцикловых характеристик. Байтовые характеристики, 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 байтового дифференциала есть сумма вероятностей всех входящих в него байтовых характеристик.

В работе [7] японские криптоаналитики определяют вероятность *i*-циклового усеченного дифференциала следующим образом

$$P_{\text{бд}}^{(i)}(\beta'(0),\beta'(i)) = P(\chi(\Delta X(i)) = \\ = \beta'(i) \,|\, \chi(\Delta X(0)) = \beta'(0)),$$

где χ – функция-характеристика; $\beta' = \chi(\beta(i))$, а $\beta(i)$ – возможная дифференциальная разность на выходе i-го нелинейного уровня; $\Delta X\ (0)$ – входная разность; $\Delta X(i)$ – разность на выходе $(i+1)$-го цикла.

Как следует из [5, 6], наличие *r*-циклового эффективного байтового дифференциала позволяет организовать атаку на *r*-цикловый, а в некоторых случаях и на $(r+1)$-цикловый шифр.

Напомним также, что байтовая дифференциальная характеристика или байтовый дифференциал считаются *эффективными*, когда вероятность $p_{\text{бд}}$ или $P_{\text{бд}}$ 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):

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

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

Если удается найти эффективный дифференциал, то обычно на последнем цикле, где известны выходное значение разности (значения криптограмм) и входной вектор активизации (в соответствии с используемым байтовым дифференциалом). Эта информация позволяет получить информацию о подключе последнего цикла.

В основе выполнения оценки стойкости бсш к атаке усеченных дифференциалов обычно лежит поиск эффективных байтовых дифференциалов, покрывающих достаточное для построения атаки число циклов и обладающих достаточно высокой вероятностью.

В работе [2] для шифра rijndael доказана лемма о числе активных колонок в двух последовательных циклах шифра. Согласно с этой леммой, суммарное количество активных колонок на входе и выходе двух циклов преобразований составляет не менее 5.

Используя эту лемму, покажем, что для шифра FIPS-197 (rijndael со 128-битным блоком) справедлива следующая теорема.

Теорема 1. Для шифра FIPS-197 не существует эффективных байтовых дифференциальных характеристик (БДХ) для 3 и более циклов.

Доказательство. Рассмотрим 3-цикловую БДХ для такого шифра. Пусть на входе 1-го, 2-го и 3-го цикла будет, соответственно, a, b и c активных колонок ($a > 0$, $b > 0$ и $c > 0$). В первом цикле после операции MC в каждой активной колонке должно быть не более b активных байтов (в противном случае во втором цикле будет больше, чем b активных колонок). Тогда, учитывая, что каждый пассивный байт на выходе преобразования MC уменьшает вероятность БДХ примерно в 2^8 раз, верхняя граница вероятности БДХ после первого цикла составит

$$2^{-(4-b)\cdot 8a}.$$

Исходя из аналогичных соображений, после двух циклов вероятность БДХ составит не более, чем

$$2^{-(4-b)\cdot 8a} \cdot 2^{-(4-c)\cdot 8b},$$

при этом, если считать, что в третьем цикле после преобразования мс в каждой из c активных колонок будут активны все байты, то, используя выражение (1) для вычисления нижней границы вероятности эффективной бдх, будет получено

$$p_{\text{сл}} = 2^{-(4-c)\cdot 32}.$$

Для того, чтобы теорема была справедлива, должно выполняться неравенство

$$2^{-(4-b)\cdot 8a} \cdot 2^{-(4-c)\cdot 8b} \le 2^{-(4-c)\cdot 32}. \qquad (2)$$

Следует отметить, что каждый дополнительный пассивный байт на выходе операции мс третьего цикла будет добавлять множитель 2^{-8} в обе части этого неравенства.

Неравенство (2) равносильно неравенству

$$-(4-b)\cdot 8a - (4-c)\cdot 8b \le -(4-c)\cdot 32. \qquad (3)$$

В соответствии с леммой о числе активных колонок ([2]) можно записать $a + c \ge 5$, поскольку $4 \ge b$, то $(4-b) \ge 0$, а следовательно, $-(4-b)\cdot 8a \le 0$, поэтому в выражение (3) можно подставить вместо a минимальное значение, т.е. сделать замену $a = 5 - c$, раскрыв после этого в (3) скобки и выполнив элементарные преобразования, приходим к равносильному неравенству

$$8b \le 32,$$

которое является справедливым, так как в соответствии с утверждением $b < 4$ теорема доказана.

Справедливость доказанной теоремы подтвердилась в ходе вычислительных экспериментов по

поиску эффективных БДХ с использованием метода Мораи [8] и с использованием метода, предложенного в работе [9]. Результаты поиска представлены в табл. 1.

Таблица 1

Размер блока шифра, биты	Число колонок в блоке	Макс. число циклов	Макс. вер. БДХ, $p_{бд}$	$p_{бд}/p_{сл}$
128	4	2	$\approx 2^{-8}$	1,68e+07
192	6	3	$\approx 2^{-16}$	62991
256	8	5	$\approx 2^{-80}$	60101

Исходя из полученных в ходе вычислительных экспериментов данных, вероятно, что для вариантов шифра rijndael с размером блока 192 и 256 битов может быть доказана аналогичная теорема об отсутствии эффективных БДХ для 4 и 6 циклов, соответственно.

Основным итогом работы стало обоснование отсутствия эффективных БДХ для шифра rijndael-128 с числом циклов 3 и более. Из этого следует, что шифр AES с еще одним дополнительным циклом (4 и более циклов) является защищенными от атаки усеченных (байтовых) дифференциалов.

Литература

[1] National Institute of Standards and Technology «Advanced encryption algorithm (AES) development.» // FIPS 197, U.S. Department of Commerce, Nov. 2001.

[2] *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.

[3] *L. R. Knudsen*. Truncated and Higher Order Differentials. In B. Preneel, editor, Fast Software Encryption — Second International Workshop, Volume 1008 of Lecture Notes in Computer Science, pp. 196–211. Springer-Verlag, Berlin, Heidelberg, New York, 1995.

[4] *K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita*. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms, Selected Areas in Cryptography – 7th Annual International Workshop, SAC2000, Lecture Notes in Computer Scienca 2012, pp. 39-56, Springer-Verlag, Berlin, 2001.

[5] *L. R. Knudsen, T. A. Berson*. Truncated differentials of SAFER, 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] *M. Matsui, T. Tokita*. Cryptanalysis of reduced version of the block cipher E2, in pre-proceedings of Fast Software Encryption'99, pp. 70-79, 1999.

[7] *M. Sugita, K. Kobara*. 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.

[8] *S. Moriai, M. Sugita, K. Aoki*. Security of E2 against Truncated Differential Cryptanalysis. In H. Heys and C. Adams, editors, Selected Areas in Cryptography — 6th Annual International Workshop, SAC'99, Volume 1758 of Lecture Notes in Computer Science, pp. 106–117, Berlin, Heidelberg, New York, Springer-Verlag, 2000.

[9] *Руженцев В.И.* О методах оценки стойкости к атаке усеченных дифференциалов // Радиоэлектроника и информатика. 2003. №4. С. 130-133.

Поступила в редколлегию 12.09.2008

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

Олейников Роман Васильевич, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.