УДК 681.3.06: 519.248.681

В.И. РУЖЕНЦЕВ, канд. техн. наук

ПРО ДОКАЗАТЕЛЬСТВО ОТСУТСТВИЯ ЭФФЕКТИВНЫХ БАЙТОВЫХ ДИФФЕРЕНЦИАЛЬНЫХ ХАРАКТЕРИСТИК ДЛЯ RIJNDAEL-ПОДОБНЫХ ШИФРОВ

Вопросы криптостойкости американского стандарта шифрования FIPS-197 [1] (AES или Rijndael [2]) вызывают интерес у многих криптографов. В работе [3] представлено обоснование стойкости этого алгоритма блочного симметричного шифрования к атаке усеченных (байтовых) дифференциалов. Однако позже были выявлены некоторые неточности в доказательстве одной из представленных в [3] теорем. В соответствии с этой теоремой определялось минимальное количество циклов, при котором для вариантов шифра rijndael со 128-, 192- и 256-битным блоками не существуют эффективные байтовые дифференциальные характеристики.

Цель настоящей работы – устранение неточностей и представление нового варианта доказательства теоремы, а также демонстрация результатов вычислительных экспериментов, которые подтверждают справедливость теоретических выводов, представленных в этой работе и в [3].

Методика реализации атаки усеченных дифференциалов 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.

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 [5], 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 [6,7].

Основываясь на [7 – 9], 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 $\chi(x) = \chi(x0, x1, \ldots, xm) = (\chi(x0), \chi(x1), \ldots, \chi(xm))$.

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 векторы 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

$$p_{бд}^{(1)}(\delta x, \delta y) = \frac{\sum_{\substack{\chi(\Delta x)=\delta x \\ \chi(\Delta y)=\delta y}} \Pr[F(x) \oplus F(x+\Delta x) = \Delta y]}{\#\{\Delta x \in \{0,1\}^{nm} \mid \chi(\Delta x) = \delta x\}}.$$

Совокупность значений входного и выходного векторов активизации для одного цикла преобразований называется *одноцикловой байтовой характеристикой*. Такая связь характеризуется вероятностью, которую будем обозначать как $p_{бд}^{(1)}(\delta x, \delta y)$, 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 характеристики 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 [8] японские криптоаналитики определяют вероятность i-циклового усеченного дифференциала так:

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

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 [6, 7], 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 *рбд* или *Рбд* 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):

$$Рбд > рсл \text{ или } рбд > рсл, \quad (1)$$

где $рсл \approx \left(2^{-8}\right)^u$, u – число неактивных байтов в выходной разности или число нулевых битов в выходном векторе активизации. Следует отметить, что для эффективного байтового дифференциала (эффективной байтовой характеристики) непременно будет выполняться и традиционное для обычных дифференциалов ограничение: $Рбд > 2{-}n$ ($рбд > 2{-}n$), 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.

Представленную в работе [3] лемму 1 следует переформулировать. Вместо представленной в [3] формулировки:

«Для Rijndael-подобного шифра с *k* колонками в блоке нет эффективных байтовых дифференциальных характеристик с *k* или более активными колонками на входе преобразований MixColumns»,

справедливой следует считать

«Для Rijndael-подобного шифра с *k* колонками в блоке, эффективная байтовая дифференциальная характеристика не может содержать ни одного цикла, в котором были бы активными все *k* колонок на входе преобразования MixColumns».

Доказательство леммы [3] выполнено именно для новой формулировки.

Такая формулировка затрудняет возможность определения граничного количества циклов для существования эффективных БДХ, так как для 128-битного rijndael, например, можно сколько угодно циклов подряд держать лишь три активные колонки на входе MixColumns. Такая формулировка дает возможность доказать отсутствие эффективных БДХ для тех случаев, когда количество колонок в блоке 1 или 2. Для определения граничного количества циклов для большинства вариантов шифра нужно прибегнуть к вычислительным экспериментам по поиску эффективных БДХ с использованием, например, методики из [3], модифицированной для SPN-шифров. Для размера же блока 128 битов (4 32-битовые колонки в блоке) в этой работе представлен новый вариант доказательства отсутствия эффективных БДХ.

В работе [2] для шифра rijndael доказана лемма о числе активных колонок в двух последовательных циклах шифра. Согласно этой лемме, 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. Для шифра FIPS-197 не существует эффективных байтовых дифференциальных характеристик (БДХ) для трех и более циклов.

Доказательство. Рассмотрим трехцикловую БДХ для такого шифра. Пусть на входе MC-преобразования 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 на входе MC). Тогда, учитывая, что каждый пассивный байт на выходе преобразования MC уменьшает вероятность БДХ примерно в 28 раз, верхняя граница вероятности БДХ после первого цикла составит

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

На основе 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 MC в каждой из *c* активных колонок будут активны все байты, то, используя выражение (1) для вычисления нижней границы вероятности эффективной БДХ, можно получить $рсл = 2^{-(4-c)\cdot 32}$.

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 MC 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 [9] и метода, предложенного в работе [10]. Результаты поиска для шифров с полным набором преобразований во всех, включая последний, циклах представлены в таблице:

Размер блока шифра, биты	Число колонок в блоке	Максимальное число циклов	Максимальная вероятность БДХ, *рбд*	*рбд/рсл*
128	4	2	≈ 2–8	1,68e+07
192	6	3	≈ 2–16	62991
256	8	5	≈ 2–80	60101

Из полученных в ходе вычислительных экспериментов данных понятно, что для вариантов шифра rijndael с размером блока 192 и 256 битов может быть доказана аналогичная теорема (аналог теоремы 1 из [3]) об отсутствии эффективных БДХ для 4 и 6 циклов соответственно.

Дальнейший ход доказательства отсутствия эффективных байтовых дифференциалов, представленный в [3], остается прежним.

Основным итогом работы стало обоснование отсутствия эффективных БДХ для шифра rijndael-128 с числом циклов 3 и более. Используя представленные в [3] аргументы, можно утверждать, что шифр AES с еще одним дополнительным циклом (4 и более циклов) является защищенными от атаки усеченных (байтовых) дифференциалов.

Список литературы: 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 CD-1: Documentation, National Institute of Standards and Technology, Aug 1998. See http://www.nist.gov/aes. 3. *Руженцев, В.И.* Доказуемая стойкость rijndael-подобных шифров к атаке усеченных дифференциалов // Радіоелектронні і комп’ютерні системи. – 2012. – №5. – С. 51-55. 4. *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. 5. *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. 6. *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. 7. *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. 8. *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. 9. *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. 10. *Руженцев, В.И.* О методах оценки стойкости к атаке усеченных дифференциалов // Радиоэлектроника и информатика. – 2003. – №4. – С. 130-133.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 09.09.20012