ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 681.3.06: 519.248.681

О МЕТОДЕ ВЫПОЛНЕНИЯ ОЦЕНКИ СТОЙКОСТИ ШИФРА RIJNDAEL К ДИФФЕРЕНЦИАЛЬНЫМ АТАКАМ

ДОЛГОВ В.И., РУЖЕНЦЕВ В.И.

Исследуется предложенная в работе [1] методика выполнения оценки стойкости шифра Rijndael к дифференциальным атакам. Описываются результаты тестирования стойкости алгоритма с использованием предлагаемой в [1] методики, а также отмечаются ее недостатки.

На сегодняшний день актуальными являются задачи защиты информации, обеспечения ее целостности, подлинности и конфиденциальности. Конфиденциальность в информационных системах чаще всего обеспечивается путем использования блочных симметричных шифров. Одним из основных требований к современным шифрам является стойкость к криптоаналитическим атакам, среди которых наиболее мощными считаются дифференциальный и линейный криптоанализы [6, 7].

До настоящего времени большинство методик выполнения оценок стойкости блочных симметричных шифров к атакам дифференциального криптоанализа основывалось на рассмотрении дифференциальных характеристик с максимальными вероятностями. N-цикловая дифференциальная характеристика, как известно, задает фиксированное значение дифференциальной разности на входах и выходах каждого из N циклов шифра, и вероятность дифференциальной характеристики есть произведение вероятностей прохождения разности через каждый из этих циклов. Для атаки промежуточные значения разности не важны, они важны лишь на входе первого цикла, так как в соответствии с этим значением будет производиться подбор "претендентов" на правильные пары, и на входе последнего цикла, потому что это значение непосредственно используется для получения информации о битах подключа, применяемого на последнем цикле. Поэтому для получения ответа на вопрос о возможности проведения эффективной атаки дифференциального криптоанализа следует рассматривать не столько дифференциальные характеристики, сколько дифференциалы [2], которые определяют начальную разность и разность на выходе предпоследнего цикла или, что эквивалентно, разность на входе последнего цикла. Вероятность дифференциала есть сумма вероятностей всех дифференциальных характеристик, имеющих определенные значения входной и выходной разностей. Следовательно, переход от рассмотрения дифференциальных характеристик к рассмотрению дифференциалов, безусловно, позволяет получить более адекватные оценки стойкости рассматриваемых шифров к дифференциальному криптоанализу.

Приведенные соображения в полной мере относятся и к одному из наиболее перспективных на сегодня шифров – блочному симметричному шифру Rijndael [5]. Авторы этого шифра выполняли оценку стойкости к дифференциальным атакам путем подсчета минимально возможного числа активных S-блоков в дифференциальных характеристиках, а это, по сути, и есть поиск дифференциальной характеристики с наибольшей вероятностью. В работе [1] предложен новый метод выполнения оценки стойкости особого типа блочных шифров к атакам дифференциального криптоанализа, основанный на рассмотрении дифференциалов. Целью настоящей работы является изучение и исследование предложенного японскими учеными метода оценки стойкости шифра Rijndael к дифференциальным атакам.

Коротко остановимся на основных моментах, изложенных в работе [1]. Авторы рассматривают процедуры оценки вероятностей усеченных и обычных дифференциалов. Следует отметить, что само по себе наличие дифференциала с вероятностью выше пороговой не является достаточным условием для реализации эффективной атаки. На примере классической дифференциальной атаки можно сказать, что не менее важной составляющей является процедура отбора правильных пар или, более точно, метод, при помощи которого можно отличить правильную пару от неправильной.

В основе предложенного метода оценки вероятностей дифференциалов различных типов лежит концепция байт-ориентированных шифров со случайными выходными дифференциалами. Приведем два определения из работы [1].

Определение 1 ([1]). Байт-ориентированное преобразование

$$Y = g(X, Z),$$

$$(X = (X_1, X_2, ..., X_m) \in GF(2^n)^m,$$
$$Y = (Y_1, Y_2, ..., Y_m) \in GF(2^n)^m,$$
$$Z = (Z_1, Z_2, ..., Z_{m'}) \in GF(2^n)^{m'})$$

называется преобразованием со случайными дифференциалами, если для любой входной разности a справедливо следующее выражение:

$$P(\Delta Y = \beta \mid \Delta X = a) = p^{h(\chi(\beta))} P(\chi(\Delta Y) = \chi(\beta) \mid \Delta X = a)),$$

где ключи выбираются случайно; $h(f)$ – вес Хемминга аргумента f; χ - функция-характеристика, ставит 1 на месте активных S-блоков в аргументе и 0 – в противном случае; $p = \frac{1}{2^n - 1}$; $\Delta X = (\Delta X_1, \Delta X_2, ..., \Delta X_m)$ и $\Delta Y = (\Delta Y_1, \Delta Y_2, ..., \Delta Y_m)$

есть, соответственно, входная и выходная дифференциальные разности.

Определение 2 ([1]). Байт-ориентированный шифр с цикловой функцией $X(i+1) = f(X(i), Z(i+1))$ (i=0,1,...,r-1), где $Z(i)$ (i = 0,1,...,r-1) – подключи, называется шифром со случайными дифференциалами, если для любого преобразования со случайными дифференциалами $X(0) = g(X, Z(0))$ производное преобразование $X(1) = f(g(X, Z(0)), Z(1))$ также является преобразованием со случайными дифференциалами.

В соответствии с приведенными определениями S-подстановку алгоритма Rijndael авторы относят к преобразованиям со случайными дифференциалами. Однако нельзя сказать, что S-блок шифра Rijndael полностью подходит под определение 1, так как, в соответствии с таблицей дифференциальной разности, не все выходные разности для фиксированного значения входной разности равновероятны: для каждого входного значения разности одно из выходных значений является более вероятным (2/255), а остальные выходные значения появятся с вероятностью 1/255. К примеру, если на входе S-блока разность 01, то с вероятностью 2/255 выходная разность будет равняться 01, с вероятностями 1/255 появятся другие возможные ненулевые выходные разности. Таким образом, шифр Rijndael можно отнести к шифрам со случайными дифференциалами лишь в некотором приближении.

Далее, авторы, принимая во внимание работу [3], определяют вероятность усеченного дифференциала для SPN-структуры:

$$P'_i(\beta'(i), \beta'(0)) = P(\chi(\Delta X(i)) = \beta'(i) \mid \chi(\Delta X(0)) = \beta'(0), \Delta X = a),$$

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

Исходя из приведенных определений, японские криптоаналитики приходят к такой рекурсивной процедуре вычисления вероятности усеченного дифференциала:

$$P'_i(\beta'(i), \beta'(0)) = \sum_{\beta'(i-1)} N(P, \beta'(i), \beta'(i-1)) p^{h(\beta(i-1))} \times \times P'_{i-1}(\beta'(i-1), \beta'(0)).$$

Здесь значение функции $N(P, \gamma, \delta)$ для матрицы P размером $m \times m$ над полем $GF(2^n)$, и $\gamma, \delta \in GF(2)^m$ определяется так:

$$N(P, \gamma, \delta) = \#\{(\Delta X, \Delta Y) \in \left(GF(2^n)^m\right)^2 / \{0\} \mid \Delta Y = P\Delta X, \chi(\Delta X) = \gamma, \chi(\Delta Y) = \delta\},$$

$p = \frac{1}{2^n - 1}$; $\beta'(i) = \chi(\beta(i))$, а $\beta(i)$ – возможная дифференциальная разность на выходе i-го нелинейного уровня; ΔX – входное в цикловую шифрующую функцию значение разности; ΔY – значение разности на выходе цикловой шифрующей функции.

Опираясь на описание атаки усеченных дифференциалов из работы [3], следует заметить, что эффективная атака возможна лишь в том случае, когда вероятность усеченного дифференциала не только выше, чем 2^{-128}, но и больше, чем пороговая вероятность – вероятность получения на выходе той же комбинации активных байтов при произвольной комбинации активных байтов на входе (вычисляется как $\left(2^{-8}\right)^{na}$, где na – число неактивных байтов в выходной разности). Поскольку для вероятности усеченных дифференциалов вводится это дополнительное ограничение, то вводится и дополнительный показатель: отношение вероятности к пороговой вероятности, а значение этого показателя должно быть больше 1.

Вероятность же обычного дифференциала связана с вероятностью усеченного следующим соотношением: $P_i(\beta(i), a) = p^{h(\beta'(i))} P_i'(\beta'(i), a')$.

Из этого соотношения видно, что вероятность обычного дифференциала зависит от значения дополнительного показателя усеченного дифференциала. Чем выше этот показатель для усеченного дифференциала, тем выше вероятность соответствующего обычного дифференциала, а если вероятность усеченного дифференциала будет ниже пороговой (значение дополнительного показателя меньше 1), то вероятность обычного дифференциала будет ниже, чем 2^{-128}. Видно также, что для каждого активного S-блока все 255 возможных значений разности принимаются равновероятными. А в этом случае и все возможные значения подключа будут равновероятны. Поэтому возникает вопрос о возможности проведения классической атаки дифференциального криптоанализа [6], даже если найденный по предложенной японскими учеными методике дифференциал обладает достаточно высокой вероятностью (выше, чем 2^{-128}).

Изложенный метод оценки вероятности усеченных и обычных дифференциалов был реализован программно. При помощи этого метода было проведено тестирование 128-битного шифра Rijndael[1]. Результаты тестирования показали, что максимальное число циклов, для которого существуют эффективные усеченные дифференциалы, – 3. В таблице представлены два эффективных 3-цикловых усеченных дифференциала, первый из которых обладает лучшей вероятностью, а второй – лучшим значением дополнительного показателя.

На основании полученных результатов можно сделать вывод о том, что обычная дифференциальная атака и атака усеченных дифференциалов не опасны для шифра Rijndael с 5 и более циклами.

К недостаткам предлагаемой методики следует отнести ее высокую вычислительную сложность, которая растет экспоненциально с ростом числа циклов. Как следствие – методика применима для небольшого числа циклов (оценить вероятности

[1] В последнем цикле отсутствует операция MixColumn.

3-цикловые усеченные дифференциалы[2]

№	Характ. вх. разности				Характ. вых. разности.				Вер. усеч. дифф.	Доп. показ.	Вер. обычн. дифф.
1	0	0	0	0	0	1	1	1	2^{-8}	1.66e+7	2^{-104}
	0	0	0	0	1	0	1	1			
	0	1	0	0	1	1	0	1			
	1	0	0	0	1	1	1	0			
2	0	0	0	1	1	0	0	0	2^{-24}	4.56e+21	2^{-56}
	0	0	1	0	0	1	0	0			
	0	1	0	0	0	0	1	0			
	1	0	0	0	0	0	0	1			

дифференциалов с 5 и более циклами не удалось). Естественно, что процедура поиска эффективных усеченных дифференциалов на основе такого метода вычисления вероятностей будет работать для еще меньшего числа циклов.

Следует также отметить, что предложенная методика не всегда применима для дифференциалов с небольшим числом циклов (1 или 2), так как получаемые результаты не являются верными. Рассмотрим один полный цикл шифра Rijndael. Пусть входная разность содержит один активный S-блок. Тогда на выходе возможны 256 вариантов разности с 4 активными блоками. Один из этих вариантов более вероятен, и его вероятность составит $2/255 \approx 2^{-7}$. Если рассчитать вероятность такого дифференциала по предлагаемой методике, то получится $\approx 2^{-32}$.

С помощью предложенной японскими учеными методики был произведен также поиск невозможных дифференциалов (impossible differentials). Найдены 4-цикловые невозможные дифференциалы, содержащие входную разность с одним активным S-блоком и выходную разность с одновременно неактивными S-блоками хотя бы в одной из перечисленных комбинаций: 1,6,11,16; 2,7,12,13; 3,8,9,14 или 4,5,10,15. Как оказалось, эти невозможные дифференциалы были обнаружены Э. Бихамом и использованы в предложенной им атаке на 5-цикловый Rijndael [4].

Таким образом, исследование метода оценки стойкости шифра Rijndael к атакам дифференциального криптоанализа, предложенного японскими учеными, подтвердило стойкость шифра Rijndael со стандартным числом циклов к дифференциальным атакам. С другой стороны, выявлены некоторые недостатки предлагаемого метода. К ним следует отнести неточность результатов, получаемых при тестировании шифра с небольшим числом циклов. Кроме того, сложность вычислений, выполняемых в соответствии с предлагаемым методом, резко возрастает с увеличением числа циклов шифра, как следствие – тестирование шифра с 5 и более циклами представляется проблематичным. При исследовании метода были выявлены некоторые неточности его обоснования и поставлены новые вопросы, поиск ответов на которые станет предметом дальнейших исследований.

[2] Характеристика разности отражает активность (1) или неактивность (0) S-блоков (байтов).

Литература: 1. *Makoto Sugita, Kazukuni 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. 2. *Lai X., Massey J.L., Murphy S.* Markov ciphers and differential cryptanalysis, Advanced in Cryptology, Proceeding Eurocrypt'91, LNCS 547 / D.W. Davies, Ed., Springer-Verlag, 1991. P. 17-38. 3. *Matsui M., Tokita T.* Cryptanalysis of a Reduced Version of the Block Cipher E2. / 6–th international workshop, preproceedings FSE'99. 4. *Biham E., Keller N.* Cryptanalysis of reduced variants of Rijndael. / http://csrc.nist.gov/encryption/aes/ round2/ conf3/papers/35-ebiham.pdf. 5. *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. 6. *Biham E., Shamir A.* Differential Cryptanalysis of the DES-like Cryptosystems, Journal of Cryptology. 1991. Vol. 4. P. 3-72. 7. *Matsui M.* Linear Cryptanalysis Metod for DES Cipher / Pros. Eurocrypt'93. Norway. 1993. P. 386-397.

Поступила в редколлегию 19.11.2001

Рецензент: д-р техн. наук, проф. Горбенко И.Д.

Долгов Виктор Иванович, д-р техн. наук, профессор кафедры БИТ ХНУРЭ. Научные интересы: криптография, защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-94-25.

Руженцев Виктор Игоревич, аспирант кафедры БИТ ХНУРЭ. Научные интересы: криптография, защита информации. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 40-94-25.

УДК 681.518;51;330; 330.4;330.46

ДВУМЕРНАЯ МОДЕЛЬ КООПЕРАЦИОННЫХ ВЗАИМОДЕЙСТВИЙ В ЭКОНОМИКЕ

ЖУРАВКА А.В., МОСКОВКИН В.М., БРУК В.В.

По аналогии с известной двумерной моделью конкурентных взаимодействий в популяционной экологии предлагается модель кооперационных взаимодействий, интерпретированная в рамках кооперации двух экономических объектов.

Нами в работе [1] известная двумерная модель конкурентных взаимодействий в популяционной экологии [2,3] была интерпретирована в рамках конкурентных взаимодействий двух экономических объектов. В настоящей работе мы предлагаем заменить знаки "минус" в нелинейных членах, описывающих конкуренцию, на знаки "плюс" и тем самым перейти к анализу кооперационных взаимодействий двух экономических объектов. Новая динамическая система второго порядка в обозначениях работы [1] будет выглядеть следующим образом:

$$\begin{aligned} \frac{dX_1}{dt} &= (a - bX_1 + \delta X_2)X_1, \\ \frac{dX_2}{dt} &= (c - \gamma X_1 + dX_2)X_2. \end{aligned} \qquad (1)$$

В этой динамической системе первые три особые точки совпадают с особыми точками в случае конкурентных взаимодействий. Все особые точки системы уравнений (1) имеют вид: 1. (0,0); $2.\left(0, \quad \frac{c}{d}\right); 3.\left(\frac{a}{b}, \quad 0\right); 4.\left(\frac{ad + \delta c}{bd - \gamma\delta}, \quad \frac{bc + a\gamma}{bd - \gamma\delta}\right).$