1) $p_1 = 1$ и $p_i = p_{i-1} - \dfrac{1}{2 \cdot 4^{i-2}}$ при $2 \leqslant i \leqslant n$;
2) $\mathrm{adp}^{\oplus}(\alpha, \beta, \gamma) = p_i \iff$ тройка (α, β, γ) получается из тройки $(0, 2^{n-i}, 2^{n-i})$ композицией следующих преобразований, сохраняющих значение $\mathrm{adp}^{\oplus}$ [8]:
   а) перестановка элементов тройки;
   б) $(\alpha, \beta, \gamma) \mapsto (\alpha \oplus 2^{n-1}, \beta \oplus 2^{n-1}, \gamma)$;
   в) $(\alpha, \beta, \gamma) \mapsto (\pm\alpha, \pm\beta, \pm\gamma)$, где $\pm\alpha$ обозначает α или $-\alpha \bmod 2^n$.

Замечание 1. Если $\mathrm{adp}^{\oplus}(\alpha, \beta, \gamma) \neq p_i$ для $1 \leqslant i \leqslant n$ из теоремы 2, то

$$\mathrm{adp}^{\oplus}(\alpha, \beta, \gamma) \leqslant 1/4.$$

Из теоремы 2 нетрудно получить количество разностей, на которых достигаются данные максимальные значения. Обозначим количество разностей (α, β, γ), $\alpha, \beta, \gamma \in \in \mathbb{Z}_2^n$, на которых достигается $\mathrm{adp}^{\oplus}(\alpha, \beta, \gamma) = p_i$, как C_i.

Следствие 2. Для C_i верны следующие утверждения:
— $C_1 = 4$, $C_2 = 24$;
— $C_3 = C_4 = \ldots = C_n = 48$.

ЛИТЕРАТУРА

1. *Shimizu A. and Miyaguchi S.* Fast data encipherment algorithm FEAL // LNCS. 1988. V. 304. P. 267–278.
2. *Wheeler D. J. and Needham R. M.* TEA, a tiny encryption algorithm // LNCS. 1995. V. 1008. P. 363–366.
3. *Bernstein D. J.* Salsa20 specification. eSTREAM Project algorithm description. `http://www.ecrypt.eu.org/stream/salsa20pf.html`. 2005.
4. *Beaulieu R., Shors D., Smith J., et al.* The SIMON and SPECK Families of Lightweight Block Ciphers. `https://eprint.iacr.org/2013/404`.
5. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
6. *Mouha N., Velichkov V., De Cannière C., and Preneel B.* The differential analysis of S-functions // LNCS. 2011. V. 6544. P. 36–56.
7. *Lipmaa H. and Moriai S.* Efficient algorithms for computing differential properties of addition // LNCS. 2002. V. 2355. P. 336–350.
8. *Mouha N., Kolomeec N., Akhtiamov D., et al.* Maximums of the additive differential probability of Exclusive-Or // IACR Trans. Symmetric Cryptology. 2021. No. 2. P. 292–313.

УДК 519.7 DOI 10.17223/2226308X/15/15

НЕКОТОРЫЕ УСЛОВИЯ ПРИМЕНИМОСТИ ИНТЕГРАЛЬНОГО МЕТОДА К ЧЕТЫРЁМ РАУНДАМ AES-ПОДОБНЫХ АЛГОРИТМОВ

К. Н. Панков

Получен ряд необходимых и одно достаточное условие того, что к блочным алгоритмам, построенным аналогично алгоритму AES (например, SQUARE, Rijndael, Crypton) с уменьшенным до четырёх числом раундов может быть применён интегральный метод криптоанализа. Приведены данные экспериментов о применении интегрального метода к алгоритму Rijndael.

Ключевые слова: *блочные алгоритмы, AES, SQUARE, Rijndael, Crypton, спектральные коэффициенты, интегральный метод.*

Современное состояние систем защиты информации характеризуется наличием так называемого квантового вызова. Появление квантового компьютера с соответствующим набором характеристик, которые, согласно мнению ряда экспертов, будут достигнуты в ближайшее десятилетие, приведёт к потере некоторыми существующими системами защиты информации или отдельными их элементами своего практического значения. Таким образом, актуальной становится задача разработки, исследования и программно-аппаратной реализации криптографических примитивов, которые смогут противостоять квантовому вызову. В настоящее время существует несколько подходов к решению данной проблемы, одним из которых является использование симметричных криптографических систем, стойкость которых понизится с появлением гипотетического квантового вычислителя незначительно. Поэтому продолжает оставаться актуальным вопрос об оценке криптографической стойкости симметричных шифрсистем, применяемых как в современных информационно-телекоммуникационных системах, так и в системах интернета вещей (IoT). Отметим, что, согласно информации, приведённой в [1, 2], в условиях ограниченных ресурсов в системах IoT наиболее рационально использовать алгоритмы блочного шифрования. В соответствии с [3] одним из основных методов криптоанализа подобных алгоритмов является интегральный метод.

Интегральный метод, впервые названный так в [4], предложен в работе [5] и является развитием метода из [6]. Этот метод ещё называют square-атака [5] или saturation-атака [7] (метод квадрата и метод статистического насыщения). Он аналогичен по схеме применения известному дифференциальному методу, также являясь атакой на основе адаптивно подобранного открытого текста [8].

Общую схему метода можно описать следующим образом. Преобразование F_k, реализуемое блочным алгоритмом шифрования и зависящее от ключа k, представляется как композиция двух отображений $F_k = F_k^2 \circ F_k^1$. Допустим, что имеется такое множество $I \subset X$ блоков открытого текста, что «интеграл» $\sum\limits_{x \in I} F_k^1(x)$ обладает определённым легко проверяемым «отличительным» свойством (например, равен нулевому вектору). Предположим, что известны пары «открытый — шифрованный текст» $(x, F_k(x))$ для всех $x \in I$. Тогда для любого k можно определить элемент $\sum\limits_{x \in I} \left(F_k^2\right)^{-1}(F_k(x))$, который при истинном варианте k должен обладать «отличительным» свойством «интеграла».

Применению различных модификаций интегрального метода к ряду блочных шифрсистем, поиску путей развития этого метода и изучению связанных с ним характеристик посвящён ряд работ [9 – 12].

Интегральный метод в основном применяется к блочным алгоритмам с малым числом раундов, например к редуцированным вариантам AES [13] или Кузнечика [14], что является актуальным именно в условиях низкоресурсной криптографии.

Рассмотрим вопрос об условиях возможности применения интегрального метода к системам шифрования типа AES (алгоритмы SQUARE, Rijndael, Crypton) с четырьмя итерациями $G = f_4^* \circ f_3 \circ f_2 \circ f_1$, в которой первые три итерации f_1, f_2, f_3 обычные (но, например, в первую итерацию Rijndael мы включаем прибавление к блоку открытого текста начального ключа), а последняя итерация f_4^* может отличаться (например, в Rijndael она не содержит преобразования MixColumn). Схемы примения интегрального метода к перечисленным алгоритмам рассматриваются в работах [5, 15, 16].

Промежуточный блок после третьей итерации обозначим через $E(x, k_0) = (E_0(x, k_0), \ldots, E_{15}(x, k_0))$, где k_0 — ключ начального преобразования в терминах [17]. При фиксированном k_0 его можно рассматривать в обозначениях [18] как вектор-функцию $E(x, k_0) = E_{k_0}(x) : V_{128} \to V_{128}$, $E(x, k_0) = f_3 \circ f_2 \circ f_1(x, k_0)$.

Пусть подвектор $B_i = z$, $i \in \{0, \ldots, 15\}$, принимает все возможные значения из V_8, а остальные подвекторы блока данных фиксированы. Полученное множество обозначим $I_i = \{(B_0, \ldots, B_{i-1}, z, B_{i+1}, \ldots, B_{15}) : z \in V_8\}$. Рассмотрим для каждого индекса $m \in \in \{0, \ldots, 15\}$ при фиксированном $k_0 \in V_{128}$ значение интеграла $\sum\limits_{x \in I_i} E_m(x, k_0)$.

Теорема 1. В AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций для любого непустого множества $J \subset \{1 + 8s, \ldots, 8 + 8s\}$, $s \in \{0, \ldots, 15\}$, и любого множества $I = \{1, \ldots, 128\} \setminus \{8l + k : k = 1, \ldots, 8\}$, $l \in \{0, \ldots, 15\}$, для отображения $E(\cdot, k_0)$ при фиксированном ключе $k_0 \in V_{128}$ в обозначениях [18] верно, что

$$\sum_{x \in I_i} E_m(x, k_0) = 0.$$

Следствие 1. В AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций для любого непустого множества $J \subset \{1 + 8s, \ldots, 8 + 8s\}$, $s \in \{0, \ldots, 15\}$, и любого множества $I = \{1, \ldots, 128\} \setminus \{8l + k : k = 1, \ldots, 8\}$, $l \in \{0, \ldots, 15\}$, для отображения $E(\cdot, k_0)$ при фиксированном ключе $k_0 \in V_{128}$ в обозначениях [18] верно, что

$$w_I^J(E_{k_0}(x)) \equiv 0 \pmod 2.$$

Следствие 2. В условиях следствия 1 в обозначениях [19] выполняется

$$\Delta_\varnothing^J(E_{k_0}(x)) \equiv 0 \pmod 2.$$

Предположим, что нам известно 256 пар открытого и шифрованного текстов (x, y), $x \in I_i$, $y = y(x) = G(x, k_0^*) = f_4^*(E(x, k_0), k_4) = s(E(x, k_0)) \oplus k_4$, где k_0^* — истинный ключ, а s — некоторое нелинейное преобразование, зависящее от конкретного алгоритма; ключ j-й итерации вычисляется из ключа $(j-1)$-й с помощью функции ψ: $k_j = \psi(k_{j-1})$ — нелинейной подстановки на множестве двоичных векторов V_{128}; $k_4 = \psi^4(k_0^*)$. Требуется определить ключ четвёртой итерации $k_4 = (k_{4,0}, \ldots, k_{4,15})$. Опробование ключа будем осуществлять по байтам $k_{4,0}, \ldots, k_{4,15} \in V_8$. Блок шифртекста разобьём на компоненты по 8 битов: $y(x) = (y_0(x), \ldots, y_{15}(x))$, $y_m(x) \in V_8$. Для каждого индекса $m \in \{0, \ldots, 15\}$ для каждого варианта $k_{4,m}$ вычисляем $\sum\limits_{x \in I_i} s^{-1}(y_m(x) \oplus k_{4,m})$. Если эта сумма оказывается не равной нулю, то опробуемый вариант для $k_{4,m}$ отбраковываем. Если в результате ключ определился неоднозначно, то алгоритм можно повторить для другого i.

Итак, пусть у нас имеется отображение $G : V_{128} \times V_{128} \to V_{128}$, $G = f_1 f_2 f_3 f_4^*$. При фиксированном $k_0 \in V_{128}$ отображение $G_{k_0}(x) = G(x, k_0) : V_{128} \to V_{128}$ является биективным. Очевидно, что $G(x, k_0) = s \circ E(x, k_0) \oplus \psi^4(k_0)$.

Теорема 2. Необходимым условием для того, чтобы интегральный метод позволял в AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций получить информацию о $k_{4,j}$, является то, что при любом фиксированном ключе $k_0 \in V_{128}$ для отображения $E(x, k_0) = (g_1(x), \ldots, g_{128}(x))$, где $g_m(x) : V_{128} \to V_1$, $m \in \{1, \ldots, 128\}$, существует вектор $\alpha \in V_8 \setminus \{0\}$, такой, что для любого $(\beta_1, \ldots, \beta_{120}) \in V_{120}$ в обозначениях [18] выполняется

$$\left\| (\alpha, (g_{1+8j}, \ldots, g_{8+8j}))_{i_1, \ldots, i_{120}}^{\beta_1, \ldots, \beta_{120}} \right\| \neq 128$$

для некоторого $I = \{1, \ldots, 128\} \setminus \{8j + k : k = 1, \ldots, 8\} = \{i_1, \ldots, i_{120}\}$.

Следствие 3. Необходимым условием для того, чтобы интегральный метод позволял в AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций получить информацию о $k_{4,j}$, является то, что в условиях теоремы 2 существует непустое множество $J \subset \{1+8j, \ldots, 8+8j\}$, такое, что $w_I^J\left(E(x, k_0)\right) \neq 128$.

Следствие 4. Необходимым условием для того, чтобы интегральный метод позволял в AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций получить информацию о $k_{4,j}$, является то, что в условиях теоремы 2 существует непустое множество $J \subset \{1+8j, \ldots, 8+8j\}$, такое, что $\Delta_{\varnothing}^J(E(x, k_0)) \neq 0$.

Нас интересует, в каком случае выполняется равенство

$$\mathrm{Int}\,(k_{4,j}, j) = \sum_{x \in I_i} s^{-1}(y_j(x) \oplus k_{4,j}) = 0.$$

Очевидно, что это произойдёт, если байт ключа угадан верно.

Следствие 5. Необходимым условием для того, чтобы интегральный метод позволял в AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций получить информацию о $k_{4,j}$, является то, что существуют такие $x_1, x_2 \in I_i$, $x_1 \neq x_2$, что $y_j(x_1) = y_j(x_2)$.

Теорема 3. Необходимым условием для того, чтобы интегральный метод позволял в AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций получить информацию о $k_{4,j}$ для некоторого $j \in \{0, \ldots, 15\}$, является то, что отображение s является нелинейной подстановкой.

Рассмотрим мультимножество $\{y_j(x) : x \in I_i\}$, где $(y_0(x), \ldots, y_{15}(x)) = G(x, k_0^*)$, состоящее из 256 элементов, и его подмножество (уже не являющееся мультимножеством)

$$Y_j^* = \left\{\alpha \in V_8 : |\{x \in I_i : y_j(x) = \alpha\}| = 2k-1, k \in \mathbb{N}\right\}.$$

Теорема 4. Необходимым условием для того, чтобы интегральный метод позволял в AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций получить информацию о $k_{4,j}$, является то, что множество Y_j^* не пусто.

Пусть I^* — произвольное подмножество I, такое, что $\{y_j(x) : x \in I^*\} = Y_j^*$. Очевидно, что

$$\mathrm{Int}\,(k_{4,j}, j) = \sum_{x \in I_i} s^{-1}(y_j(x) \oplus k_{4,j}) = \sum_{x \in I^*} s^{-1}(y_j(x) \oplus k_{4,j}).$$

Следовательно, можно модифицировать технику применения интегрального метода тем, что интеграл будет вычисляться по меньшему множеству I^*.

Рассмотрим отображение

$$\tau_j(k_4) = \sum_{x \in I^*} s^{-1}(y_j(x) \oplus k_{4,j}), \quad \tau_j(k_4) : V_8 \to V_8.$$

Теорема 5. Необходимым условием для того, чтобы интегральный метод позволял в AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций получить информацию о $k_{4,j}$, является то, что существует такой элемент $\alpha \in V_8$, что $\tau_j(\alpha) \neq 0$.

Теорема 6. Достаточным условием для того, чтобы интегральный метод позволял в AES-подобных схемах (SQUARE, Rijndael, Crypton) для четырёх итераций найти $k_{4,j}$, является то, что существует единственный элемент $\beta \in V_8$, такой, что $\tau_j(\beta) = 0$.

В рамках исследования интегрального метода проведено 16 наборов экспериментов для редуцированного до четырёх раундов алгоритма Rijndael по схеме из [20], в которых в качестве набора открытых текстов взято множество из 256 векторов $I_0 = \{x = (x_0, \ldots, x_{15}) \in V_{128}\}$, где x_0 принимает все значения из V_8, а остальные x_j равны нулю. На фиксированных множествах из 256 ключей $\{k_0^*\}_t$, $t \in \{1, \ldots, 16\}$, вычислялось множество шифртекстов $\{y = (y_0(x), \ldots, y_{15}(x)) = G(x, k_0^*) : x \in I_0\}$, а затем для заданного номера байта $j = j(t)$ для всех $k_{4,j} \in V_8$ вычислялся интеграл $\mathrm{Int}(k_{4,j}, j, I_0) = \sum\limits_{x \in I_0} s^{-1}(y_j(x) \oplus k_{4,j})$. Среди тех $k_{4,j}$, для которых $\mathrm{Int}(k_{4,j}, j, I_0)$ обращался в ноль, обязательно содержится истинный байт четвёртой итерации ключа, но он далеко не всегда единственен. В каждом из наборов экспериментов для каждого ключа из $\{k_0^*\}_t$ подсчитывалось, на скольких байтах $k_{4,j}$ интеграл $\mathrm{Int}(k_{4,j}, j, I_0)$ обращался в ноль. В качестве множеств $\{k_0^*\}_t = \left\{(k_{0,0}^*, \ldots, k_{0,15}^*) \in V_{128} : k_{0,l}^* \in V_8, l \in \{0, \ldots, 15\}\right\}_t$ брались векторы, у которых байт $k_{0,m}^*$ принимал все значения из V_8 при фиксированном $m = m(t) = j(t)$, а остальные байты равны нулю. Данные экспериментов сведены в таблицу, в которой приведено количество ключей из множества $\{k_0^*\}_t$, для которых интеграл $\mathrm{Int}(k_{4,j}, j, I_0)$ равен нулю на v байтах при всех $v \in \{1, \ldots, 7\}$.

t	$j(t)$	v						
		1	2	3	4	5	6	7
1	0	97	88	49	15	7	0	0
2	1	102	97	37	11	7	2	0
3	2	102	89	38	21	4	2	0
4	3	86	97	51	17	4	1	0
5	4	104	95	42	9	5	1	0
6	5	95	93	47	17	3	1	0
7	6	82	109	47	11	5	2	0
8	7	80	105	45	18	8	0	0
9	8	102	86	42	22	3	1	0
10	9	110	85	43	16	2	0	0
11	10	95	93	54	10	2	1	1
12	11	102	85	52	12	5	0	0
13	12	106	89	48	11	2	0	0
14	13	86	106	44	16	4	0	0
15	14	91	105	40	17	3	0	0
16	15	83	97	52	12	12	0	0

ЛИТЕРАТУРА

1. *Жуков А. Е.* Легковесная криптография. Ч. 1 // Вопросы кибербезопасности. 2015. № 1(9). С. 26–43.
2. *Жуков А. Е.* Легковесная криптография. Ч. 2 // Вопросы кибербезопасности. 2015. № 2(10). С. 2–10.
3. *Романченко А. М.* Метод оценивания результатов криптоанализа блочного шифра // Труды СПИИРАН. 2015. № 2(39). С. 101–108.
4. *Hu Y., Zhang Y., and Xiao G.* Integral cryptanalysis of SAFER+ // IET Electronics Let. 1999. V. 35. No. 17. P. 1458–1459.
5. *Daemen J., Knudsen L. R., and Rijmen V.* The block cipher Square // LNCS. 2002. V. 2365. P. 112–127.
6. *Lai X.* Higher order derivatives and differential cryptanalysis // Communications and Cryptography. Springer Intern. Ser. Engin. Comput. Sci. 1994. V. 276. P. 227–233.

7. *Collard B. and Standaert F.-X.* A statistical saturation attack against the block cipher PRESENT // LNCS. 2009. V. 5473. P. 195–210.
8. *Шнайер Б.* Прикладная криптография: протоколы, алгоритмы и исходный код. М.: Альфа-книга, 2019. 1024 с.
9. *Alda F., Aragona R., Nicolodi L., and Sala M.* Implementation and improvement of the partial sum attack on 6-round AES // Physical and Data-Link Security Techniques for Future Communication Systems. Lecture Notes in Electr. Eng. 2016. V. 358. P. 181–195.
10. *Сорокин М. А., Пудовкина М. А.* О почти совершенных нелинейных преобразованиях и разделяющем свойстве мультимножеств // Прикладная дискретная математика. Приложение. 2019. № 12. С. 237–239.
11. *ElSheikh M. and Youssef A. M.* Integral cryptanalysis of reduced-round tweakable TWINE // LNCS. 2020. V. 12579. P. 485–504.
12. *Hebborn P., Lambin B., Leander G., and Todo Y.* Strong and tight security guarantees against integral distinguishers // LNCS. 2021. V. 13090. P. 362–391.
13. *Knudsen L. R. and Wagner D.* Integral cryptanalysis (extended abstract) // LNCS. 2002. V. 2365. P. 112–127.
14. *Kiryukhin V. A.* Related-key attack on 5-round Kuznyechik // Математические вопросы криптографии. 2020. Т. 11. № 2. С. 53–67.
15. *Ferguson N., Kelsey J., Schneier B., et al.* Improved cryptanalysis of Rijndael // LNCS. 2000. V. 1978. P. 213–230.
16. *D'Halluin C., Bijnens G., Rijmen V., and Preneel B.* Attack on six rounds of Crypton // LNCS. 1999. V. 1636. P. 46–59.
17. *Лось А. Б., Нестеренко А. Ю., Рожков М. И.* Криптографические методы защиты информации. М.: Юрайт, 2018, 473 с.
18. *Панков К. Н.* Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // Прикладная дискретная математика. 2012. № 4(18). С. 14–30.
19. *Панков К. Н.* Уточнённые асимптотические оценки для числа (n, m, k)-устойчивых двоичных отображений // Прикладная дискретная математика. Приложение. 2017. № 10. С. 46–49.
20. *Бабенко Л. К., Ищукова Е. А.* Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006. 376 с.

УДК 519.7 + 004.056.55 DOI 10.17223/2226308X/15/16

СВОЙСТВА XS-СХЕМ, СВЯЗАННЫЕ С ГАРАНТИРОВАННЫМ ЧИСЛОМ АКТИВАЦИЙ[1]

Д. Р. Парфенов, А. О. Бахарев, А. В. Куценко, А. Р. Белов, Н. Д. Атутова

Гарантированное число активаций является важной криптографической характеристикой, позволяющей получить оценку стойкости блочного шифра к разностному криптоанализу. В работе исследован один из алгоритмов (Агиевич, 2020) поиска числа гарантированных активаций XS-схем. Предложен подход к оптимизации существующего решения с помощью метода ветвей и границ, а также анализа специальных матриц, характеризующих XS-схему. Для нескольких шифров проведены вычислительные эксперименты, которые демонстрируют существенное

[1]Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2022-281.