УДК 519.7 DOI 10.17223/2226308X/11/27

ОБ ИНТЕГРАЛЬНЫХ РАЗЛИЧИТЕЛЯХ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ, ОСНОВАННЫХ НА ОБОБЩЕНИЯХ СХЕМЫ ФЕЙСТЕЛЯ

М. А. Сорокин, М. А. Пудовкина

Интегральный метод и его модификации широко применяются для анализа известных алгоритмов блочного шифрования, например KHAZAD, PRESENT, RECTANGLE, PRINCE, HIGHT. Основу метода составляет структура мультимножества текстов, сохраняемая функцией зашифрования на некотором числе раундов и применяемая для построения интегрального различителя. В работе рассматриваются интегральные различители некоторых обобщений схемы Фейстеля. Так, описан 3-раундовый интегральный различитель алгоритма блочного шифрования PICARO. Для этого исследовано влияние небиективного s-бокса и расширяющей матрицы алгоритма PICARO на интегральные свойства мультимножества текстов в зависимости от числа раундов.

Ключевые слова: *интегральный метод, алгоритм блочного шифрования PICARO, обобщённая схема Фейстеля, небиективные s-боксы.*

В [1] для анализа XSL-алгоритмов блочного шифрования предложен интегральный метод криптоанализа. В настоящее время известны его различные модификации, например метод на основе разделяющего свойства [2], метод на основе мультимножеств [3]. Предложены атаки на такие известные алгоритмы блочного шифрования, как AES, PRESENT, DES, SIMON 32, CAMELLIA, KHAZAD, RECTANGLE, PRINCE, HIGHT и т. д. Идея интегрального метода состоит в нахождении структуры мультимножества текстов, сохраняемой на некотором числе раундов функцией зашифрования и используемой для построения интегрального различителя, с помощью которого восстанавливаются отдельные биты или целиком ключ шифрования.

Пусть $\mathbb{N}$ — множество натуральных чисел; $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; V_n — n-мерное векторное пространство над полем $\mathrm{GF}(2)$; $\mathrm{I}(A)$ — индикатор выполнения условия A; $\mathbf{0}_n$ — нулевой n-мерный вектор. Естественным образом пронумеруем векторы V_n. Вектору $(\alpha_1, \ldots, \alpha_n) \in V_n$ поставим в соответствие число $d = \sum\limits_{j=1}^{n} 2^{n-j}\alpha_j$. Для удобства далее будем использовать обозначение

$$v_d^{(n)} = \left(v_{d,1}^{(n)}, \ldots, v_{d,n}^{(n)}\right) = (\alpha_1, \ldots, \alpha_n).$$

Пусть Q — мультимножество векторов с носителем V_n, первичная спецификация [4] имеет вид $\widehat{Q} = \left[\left[\left(v_0^{(n)}\right)^{c_0}, \ldots, \left(v_{2^n-1}^{(n)}\right)^{c_{2^n-1}}\right]\right]$, где вектор $v_i^{(n)}$ встречается в Q ровно c_i раз, $c_0, \ldots, c_{2^n-1} \in \mathbb{N}_0$. *Интегралом мультимножества* Q [1] называется величина $Q^{\oplus}$, заданная условием

$$Q^{\oplus} = \bigoplus_{i=0}^{2^n-1} \left(v_i^{(n)} \cdot \tilde{c}_i\right) = \left(\bigoplus_{i=0}^{2^n-1} (v_{i,1}^{(n)} \cdot \tilde{c}_i), \ldots, \bigoplus_{i=0}^{2^n-1} (v_{i,n}^{(n)} \cdot \tilde{c}_i)\right),$$

где $\tilde{c}_i = c_i \bmod 2$ для $i = 0, \ldots, 2^n - 1$.

Говорят [1], что мультимножество Q с носителем V_n имеет:

1) интегральное свойство S, если $Q^{\oplus} = \mathbf{0}_n$;
2) интегральное свойство A, если $c_i = 1$ для каждого $i \in \{0, \ldots, 2^n - 1\}$;

3) интегральное свойство C, если существует такое единственное $i \in \{0, \ldots, 2^n - 1\}$, что $c_i \neq 0$;
4) интегральное свойство U, если мультимножество Q не имеет свойства S [3].

Очевидно, что интегральные свойства A и C подразумевают свойство S. Таким образом, для произвольного мультимножества Q однозначно определена функция $\varphi_n : Q \mapsto \{U, S\}$.

Пусть $n = mr$, $r > 1$. Вектор v_i можно рассматривать как элемент r-мерного векторного пространства над полем $\mathrm{GF}(2^m)$, т. е. $v_i^{(n)} = (u_{i,1}, \ldots, u_{i,r})$, $u_{i,j} \in \mathrm{GF}(2^m)$, $j = 1, \ldots, r$, $i = 0, \ldots, 2^n - 1$.

Пусть $i \in \{1, \ldots, r\}$ и $Q^{(i)}$ — мультимножество с носителем $\mathrm{GF}(2^m)$ и первичной спецификацией $\widehat{Q}^{(i)} = \left[\left[\left(v_0^{(m)}\right)^{b_0}, \ldots, \left(v_{2^m-1}^{(m)}\right)^{b_{2^m-1}}\right]\right]$, где $b_j = \sum\limits_{t=0}^{2^m-1} \mathrm{I}\left(u_{t,j} = v_j^{(m)}\right) c_t$ для $j = 0, \ldots, 2^m - 1$. Для мультимножества $Q^{(i)}$ аналогичным образом определяются интегральные свойства.

Мультимножеству Q ставится в соответствие упорядоченный набор мультимножеств $(Q^{(1)}, \ldots, Q^{(r)})$, для каждого из которых, в свою очередь, определено интегральное свойство. Упорядоченный набор соответствующих интегральных свойств называется вектором интегральных свойств мультимножества Q, например (A, C, C, C), если $r = 4$.

Пусть $g : V_n \times V_d \to V_n$ — раундовая функция итерационного алгоритма блочного шифрования, у которого частичная l-раундовая функция зашифрования $f^{(l)}_{(k_1,\ldots,k_l)} : V_n \to V_n$ задана условием $f^{(l)}_{(k_1,\ldots,k_l)} : \alpha \mapsto g_{k_l} \ldots g_{k_1}(\alpha)$, где $g_{k_i}(\alpha) = g(\alpha, k_i)$ для всех $k_1, \ldots, k_l \in V_d$, $\alpha \in V_n$.

Пусть Q_0 — мультимножество открытых текстов с носителем V_n и первичной спецификацией $\left[\left[\left(v_0^{(n)}\right)^{c_0}, \ldots, \left(v_{2^n-1}^{(n)}\right)^{c_{2^n-1}}\right]\right]$. При $t = 1, \ldots, l$ мультимножество Q_t таково, что элемент $g_{k_t} \ldots g_{k_1}\left(v_i^{(n)}\right)$ встречается в нём ровно c_i раз для каждого $i \in \in \{0, \ldots, 2^n - 1\}$.

Назовём *l-раундовым интегральным различителем* алгоритма блочного шифрования с раундовой функцией g такую последовательность мультимножеств

$$Q_0 = \left(Q_0^{(1)}, \ldots, Q_0^{(r)}\right), \ \ldots, \ Q_l = \left(Q_l^{(1)}, \ldots, Q_l^{(r)}\right),$$

что выполнены следующие свойства:

1) для каждого $j \in \{0, \ldots, l-1\}$ существует $i \in \{1, \ldots, r\}$, удовлетворяющее условию $\varphi_m(Q_j^{(i)}) \neq U$;
2) $\varphi_m(Q_l^{(i)}) = U$ для каждого $i \in \{1, \ldots, r\}$.

В данной работе исследуются интегральные свойства алгоритма блочного шифрования PICARO [5], основанного на схеме Фейстеля. Доказано существование 3-раундового различителя, при построении которого использованы свойства небиективного s-бокса и расширяющей матрицы, являющихся компонентами раундовой функции.

В настоящее время активно исследуются обобщения схемы Фейстеля [6–8]. Для некоторых из них построены интегральные различители для длины регистра $r \geqslant 4$. В частности, пусть справедливы следующие условия:

1) длина регистра $r = 4$;
2) функция усложнения h такова, что переводит мультимножество с вектором интегральных свойств (A, C, C, C) в мультимножество с вектором (U, U, U, U);

3) мультимножество Q_0 таково, что его вектор интегральных свойств равен

$$(A, C, C, C, C, C, C, C, C, C, C, C, C, C, C, C) .$$

Тогда вектор интегральных свойств мультимножества Q_5 равен

$$(U, U, U, U, U, U, U, U, U, U, U, U, U, U, U, U) .$$

ЛИТЕРАТУРА

1. *Knudsen L. and Wagner D.* Integral cryptanalysis // FSE 2002. LNCS. 2002. V. 2365. P. 112–127.
2. *Todo Y.* Structural evaluation by generalized integral property // EUROCRYPT 2015. LNCS. 2015. V. 9056. P. 287–314.
3. *Biryukov A. and Shamir A.* Structural cryptanalysis of SASAS // EUROCRYPT 2001. LNCS. 2001. V. 2045. P. 394–405.
4. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: Наука, 1982. 384 с.
5. *Piret G., Roche T., and Carlet C.* PICARO — a block cipher allowing efficient higher-order side-channel resistance // ACNS 2012. LNCS. 2012. V. 7341. P. 311–328.
6. *Nyberg K.* Generalized Feistel networks // ASIACRYPT 1996. LNCS. 1996. V. 1163. P. 90–104.
7. *Hoang V. T. and Rogaway P.* On generalized Feistel networks // CRYPTO 2010. LNCS. 2010. V. 6223. P. 613–630.
8. *Nachef V., Volte E., and Patarin J.* Differential attacks on generalized Feistel schemes // CANS 2013. LNCS. 2013. V. 8257. P. 1–19.