УДК 519.7

М.А. ПУДОВКИНА, А.М. СМИРНОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

АТАКА НА КЛАСС РЕДУЦИРОВАННЫХ XSL-АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

В работе анализируется класс редуцированных XSL-алгоритмов блочного шифрования с алгоритмом развертывания ключа второго порядка и матрицы линейного преобразования, у которой существует хотя бы два равных элемента в одной строке в случае 4, 5 и 6 раундов. При атаке используется подход «йо-йо», методы невозможных разностей и встречи посередине. Получены оценки трудоемкости атаки и вероятности её успеха.

Синтез современных блочных шифров осуществляется в соответствии неформально сформулированными принципами К. Шеннона: перемешивание и рассеивание. С данной точки зрения важным классом для рассмотрения являются XSL-алгоритмы блочного шифрования. Многие современные алгоритмы блочного шифрования являются XSL-алгоритмами, например, AES, «Кузнечик», MIDORI64, 3D.

Пусть $V_n(2^m)$ – n-мерное векторное пространство над полем $\mathbb{F}_{2^m}$, где $n, m \in \mathbb{N}$, $\oplus$ – операция сложения в $V_n(2^m)$, $I(A)$ – индикатор выполнения условия A, $g: V_n(2^m) \times V_n(2^m) \longrightarrow V_n(2^m)$ – раундовая функция XSL-алгоритма блочного шифрования. k – раундовый ключ из $V_n(2^m)$.

Пусть $h = ||h_{i,j}||$ – матрица в стандартном базисе порядка n над полем $\mathbb{F}_{2^m}$ линейного слоя раундовой функции g, $h^{-1} = ||h_{i,j}^{(-1)}||$ – обратная матрица в стандартном базисе порядка n над полем $\mathbb{F}_{2^m}$ линейного слоя раундовой функции g, d – число равных элементов в матрице $h^{-1} = ||h_{i,j}^{(-1)}||$, $s = (s_1, \dots, s_n) \in S(\mathbb{F}_{2^m})^n$. Для произвольного $\alpha = (\alpha_1, \dots, \alpha_n)$ раундовая функция g задается равенством

$$g(\alpha, k) = hs(\alpha \oplus k).$$

Для каждого $i \in \{1, \dots, n\}$ определим отображение $\chi_i: V_n(2^m) \longrightarrow \mathbb{F}_2$ условием

$$\chi_i(\alpha) = I(\alpha_i \neq 0).$$

Положим $\chi(\alpha) = \big(\chi_1(\alpha), \dots, \chi_n(\alpha)\big)$.

Для каждого $\varepsilon^{(i)} = \big(\varepsilon_1^{(i)}, \dots, \varepsilon_n^{(i)}\big) \in V_n(2^m)$ при $i \in \{1, \dots, n\}$, положим

$$\varepsilon_t^{(i)} = I(i = t).$$

Опишем идею атаки на редуцированный XSL-алгоритм блочного шифрования.

Очевидно, что

$$\chi(\alpha^{(1)} \oplus \alpha^{(2)}) = \chi(s(\alpha^{(1)}) \oplus s(\alpha^{(2)})) \quad (1)$$

для всех $\alpha^{(1)}, \alpha^{(2)} \in V_n(2^m)$, $s \in S(V_n(2^m))$.

Теорема 1. *Пусть* $\alpha, k \in V_n(2^m)$ *и существуют такие* $i, j_1, j_2 \in \{1, \dots, n\}$, *что элементы матрицы линейного отображения* h^{-1} *удовлетворяют условиям*

$$(h^{(-1)})_{i,j_1} = (h^{(-1)})_{i,j_2}, (h^{(-1)})_{i,j_1} \neq 0, s_{j_1} = s_{j_2}.$$

Тогда существует такое $\delta \in \mathbb{F}_{2^m}$, *что уравнение*

$$((hs)^{-1}(\alpha \oplus x \cdot \varepsilon^{(j_2)} \oplus k) \oplus (hs)^{-1}(\alpha \oplus \delta \cdot \varepsilon^{(j_1)} \oplus (\delta \oplus x) \cdot \varepsilon^{(j_2)} \oplus k))_i = 0$$

имеет 2^m *решений относительно* $x \in \mathbb{F}_{2^m}$.

Теорема 2. *Пусть* $\alpha, k \in V_n(2^m)$ *и существуют такие* $i, j_1, j_2 \in \{1, \dots, n\}$, *что элементы матрицы линейного отображения* h^{-1} *удовлетворяют условиям*

$$h_{i,j_1} = h_{i,j_2}, h_{i,j_1} \neq 0, s_{j_1} = s_{j_2}.$$

Тогда существует такое $\delta \in \mathbb{F}_{2^m}$, *что уравнение*

$$(hs(\alpha \oplus x \cdot \varepsilon^{(j_2)} \oplus k) \oplus hs(\alpha \oplus \delta \cdot \varepsilon^{(j_1)} \oplus (\delta \oplus x) \cdot \varepsilon^{(j_2)} \oplus k))_i = 0$$

имеет четное число решений относительно $x \in \mathbb{F}_{2^m}$.

На основании модификаций равенства (1), алгоритма построения невозможных разностей в [2], теорем 1 – 3 предложена атака на класс редуцированных XSL-алгоритмов блочного шифрования в случае 4,5,6 раундов. Доказано, что для 4 раундов трудоемкость атаки составляет $(2^m - 1)^2 + 2^{n(m+2)}$, для 5 раундов – $2^{m(n-1)} + 2^{nm}$, для 6 раундов –

$$7 \cdot 17^{n-2} \cdot 2^{2nm-n+2} \cdot 10^{1-n} \cdot \left(1 - \frac{n}{2^m - 1}\right)^d$$

операций зашифрования. Вероятность успеха атаки равна 1 в случае 4 и 5 раундов, 0.7 – в случае 6 раундов.

Список литературы

1. Ronjom S., Bardeh N. G., and Helleseth T.Yoyo tricks with AES // ASIACRYPT 2017. Lect. Notes Comput. Sci. 2017. V. 10624. No. 1. P. 217–243.

2. Shen X., Liu G., Sun B. and Li C. Impossible differentials of SPN-ciphers // LNS 2017. V. 10143. P. 47–63.

3. Altawy R. A meet in the middle attack on reduced round Kuznyechik. // IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, 2015.