УДК 519.7

М.А. ПУДОВКИНА, А.М. СМИРНОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

АТАКА РАЗЛИЧЕНИЯ НА КЛАСС АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ ФЕЙСТЕЛЯ

В работе рассматривается класс алгоритмов блочного шифрования на основе преобразования Фейстеля с XSL – функцией усложнения, у которых линейное преобразование задается подстановочной матрицей. Предложена атака различения, основанная на сохранение разности у композиции преобразований раундовой функции при применении перестановки фиксированных координат пары текстов. Получены оценки трудоемкости атаки и вероятность её успеха.

Рассмотрим класс алгоритмов блочного шифрования на основе преобразования Фейстеля, у которых линейное преобразование функции усложнения задается подстановочной матрицей.

Пусть $n, m \in \mathbb{N}$, $V_d(2^m)$ – d-мерное векторное пространство над полем $\mathbb{F}_{2^m}$, $d \in \mathbb{N}$; $\mathrm{I}(A)$ − индикатор выполнения условия A. Будем обозначать через h линейное преобразование функции усложнения и соответствующую ему подстановочную $(n \times n)$-матрицу в стандартном базисе над полем $\mathbb{F}_{2^m}$, $h = [\![h_{i,j}]\!]$.

Отображение $t: V_{2n}(2^m) \to V_n(2^m)$, подстановка $s = (s_1, \dots, s_n) \in S(\mathbb{F}_{2^m})^n$ и «дополненная» функцию усложнения $f_k: V_{2n}(2^m) \to V_{2n}(2^m)$ на раундовом ключе $k \in V_n(2^m)$ для каждого $\alpha = (\alpha_1, \dots, \alpha_{2n}) \in V_{2n}(2^m)$ задаются соответственно условиями

$$t: (\alpha_1, \dots, \alpha_{2n}) \longmapsto (\alpha_1, \dots, \alpha_n),$$
$$s: (\alpha_1, \dots, \alpha_n) \longmapsto (s_1(\alpha_1), \dots, s_n(\alpha_n)),$$
$$f_k: (\alpha_1, \dots, \alpha_{2n}) \longmapsto (hs(t(\alpha) \oplus k), \alpha_{n+1}, \dots, \alpha_{2n}).$$

Введем также линейные отображения $h_i: V_{2n}(2^m) \to V_{2n}(2^m)$, $i = 1,2$, заданные для каждого $\alpha = (\alpha_1, \dots, \alpha_{2n}) \in V_{2n}(2^m)$ условиями

$$h_1: (\alpha_1, \dots, \alpha_{2n}) \longmapsto (\alpha_{n+1}, \dots, \alpha_{2n}, \alpha_1, \dots, \alpha_n),$$
$$h_2: (\alpha_1, \dots, \alpha_{2n}) \longmapsto (\alpha_1, \dots, \alpha_n, \alpha_1 \oplus \alpha_{n+1}, \dots, \alpha_n \oplus \alpha_{2n}).$$

Пусть $g_k: V_{2n}(2^m) \to V_{2n}(2^m)$ − раундовая функция преобразования Фейстеля с «дополненной» функцией усложнения f_k на ключе $k \in V_n(2^m)$.

Лемма 1. *Для каждого* $k \in V_n(2^m)$ *справедливо равенство*

$$g_k = f_k^{-1} h_2 f_k h_1. \quad (1)$$

Равенство (1), связывающее раундовую функцию g_k и «дополненную» функцию усложнения f_k на ключе $k \in V_n(2^m)$, будет использовано при доказательстве теоремы 1, а тем самым и для построения атаки.

Для всех $\theta=(\theta_1, \dots, \theta_{2n}) \in V_{2n}(2)$, $\alpha^{(j)}=\left(\alpha_1^{(j)}, \dots, \alpha_{2n}^{(j)}\right) \in V_{2n}(2^m)$, $j = 1,2$ зададим отображение $\rho_\theta^{(i)}: V_{2n}(2^m)^2 \to \mathbb{F}_{2^m}$ условием

$$\rho_\theta^{(i)}\left(\alpha^{(1)}, \alpha^{(2)}\right)=\alpha_i^{(1)}\mathrm{I}(\theta_i = 0)+\alpha_i^{(2)}\mathrm{I}(\theta_i = 1) \text{ при } i = 1, \dots, 2n,$$

и положим

$$\rho_\theta\left(\alpha^{(1)}, \alpha^{(2)}\right)=\left(\rho_\theta^{(1)}\left(\alpha^{(1)}, \alpha^{(2)}\right), \dots, \rho_\theta^{(n)}\left(\alpha^{(1)}, \alpha^{(2)}\right)\right).$$

Из [1] вытекает равенство

$$s\left(\alpha^{(1)}\right) \oplus s\left(\alpha^{(2)}\right)=\rho_\theta\left(s(\alpha^{(1)}), s(\alpha^{(2)})\right) \oplus \rho_\theta\left(s(\alpha^{(2)}), s(\alpha^{(1)})\right)$$

для всех $\alpha^{(1)}, \alpha^{(2)} \in V_{2n}(2^m)$.

Подстановочной матрице h соответствует перестановка $\tau \in S(\{1, \dots, n\})$ координат n-мерного вектора из $V_n(2^m)$.

Теорема 1. *Пусть* $l \in \mathbb{N}$, $(k_1, \dots, k_l) \in V_n(2^m)^l$,

$$\tilde{g}_{k_1,\dots,k_l} = g_{k_l} g_{k_{l-1}} \cdots g_{k_1},$$

а τ *при разложении на независимые циклы содержит транспозицию* (r, d). *Тогда для каждой пары* $\left(\alpha^{(1)}, \alpha^{(2)}\right) \in V_n(2^m)^2$ *справедливо равенство*

$$\tilde{g}_{k_1,\dots,k_l}\left(\alpha^{(1)}\right) \oplus \tilde{g}_{k_1,\dots,k_l}\left(\alpha^{(2)}\right)=$$
$$= \tilde{g}_{k_1,\dots,k_l}\left(\rho_\theta\left(\alpha^{(1)}, \alpha^{(2)}\right)\right) \oplus \tilde{g}_{k_1,\dots,k_l}\left(\rho_\theta\left(\alpha^{(2)}, \alpha^{(1)}\right)\right),$$

где $\theta=(\theta_1, \dots, \theta_n)$,

$$\theta_i = \mathrm{I}\left(h_{i-n,d}=1, i>n \text{ или } i=d\right) \text{ при } d < n+1.$$

На основании теоремы 1 предложена атака различения, целью которой является проверка гипотезы, что подстановка $\tilde{g}_{k_1,\dots,k_l}$ не является случайной. Доказано, что трудоемкость атаки составляет 4 операции зашифрования, а вероятность успеха атаки равна 1.

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.