УДК 519.7 DOI 10.17223/2226308X/15/12

О МНОЖЕСТВАХ НЕВОЗМОЖНЫХ РАЗНОСТЕЙ АЛГОРИТМОВ ШИФРОВАНИЯ ФЕЙСТЕЛЯ С НЕБИЕКТИВНОЙ ФУНКЦИЕЙ УСЛОЖНЕНИЯ

Д. А. Захаров, М. А. Пудовкина

Рассматривается семейство l-раундовых сбалансированных алгоритмов шифрования Фейстеля с небиективной функций усложнения. Для каждого из них доказано существование l-раундовых невозможных разностей для произвольного числа раундов l, а также получена нижняя оценка числа описанных невозможных разностей. Рассматриваемому семейству принадлежит алгоритм блочного шифрования GRANULE, для которого предложен новый подход поиска невозможных разностей. Показано, что он лучше других ранее известных способов. Получено как увеличение числа l раундов, для которых находятся невозможные разности, так и их количества. Приведены аналитические оценки числа невозможных разностей, которые подтверждены экспериментально.

Ключевые слова: *алгоритм шифрования Фейстеля, невозможные разности, небиективная функция усложнения, атака различением, алгоритм шифрования GRANULE.*

Метод невозможных разностей, независимо предложенный в работах [1, 2], является одним из наиболее распространённых подходов для оценки стойкости алгоритмов блочного шифрования. Он применялся, например, для анализа алгоритмов блочного шифрования Skipjack [1], DEAL [2], Present [3], CLEFIA, Simon, Camellia, Lblock [4] и AES [5], а также для анализа семейств XSL-алгоритмов [6], алгоритмов шифрования Фейстеля [7] и обобщений алгоритма Фейстеля [8]. Кроме того, невозможные разности применяются в атаках различения [8, 9], а также для отсеивания ложных ключей в атаках, основанных на методе невозможных разностей [4, 5]. Поиск таких разностей для наибольшего числа раундов — основная задача при анализе алгоритма шифрования относительно метода невозможных разностей.

Пусть $m \in \mathbb{N}$, $m \geqslant 2$, V_m — m-мерное векторное пространство над полем GF(2) с «естественной» операцией $+$ сложения векторов, $S(X)$ — симметрическая группа на множестве X.

Определение 1. Для l-раундовой функции зашифрования $g^{(l)}\colon V_m \times K \to V_m$ с множеством ключей шифрования K пара разностей $(\varepsilon, \delta) \in V_m^2$ называется l-раундовой невозможной разностью, если для всех $(\alpha, k) \in V_m \times K$ справедливо условие

$$g_k^{(l)}(\alpha + \varepsilon) \neq g_k^{(l)}(\alpha) + \delta,$$

где $g_k^{(l)}(\beta) = g^{(l)}(\beta, k)$ для всех $(\beta, k) \in V_m \times K$.

Определение 2. Невозможной тривиальной разностью будем называть такую невозможную разность $(\varepsilon, \delta) \in V_m \times V_m$, что $\varepsilon = 0$ или $\delta = 0$.

Опишем рассматриваемое семейство сбалансированных алгоритмов Фейстеля с небиективной функцией усложнения.

Пусть A — произвольная $(m \times m)$-матрица над полем GF(2), $\operatorname{rank}(A) = m - 1$. Зафиксируем отображения $f : V_m \to V_m$, $h^{(0)} : V_m \to V_m$, $h^{(1)} : V_m \to V_m$, заданные для каждого $\alpha \in V_m$ следующими условиями:

$$f : \alpha \mapsto h^{(1)}(h^{(0)}(\alpha)); \tag{1}$$

$$h^{(1)} : \alpha \mapsto \alpha A. \tag{2}$$

Рассмотрим также отображение $\nu : V_m^2 \times V_m \to V_m^2$ с частичной функцией $\nu_k \in S(V_m^2)$:

$$\nu_k : (\alpha_1, \alpha_0) \mapsto (\alpha_0 + f(\alpha_1) + k, \alpha_1) \text{ для всех } (\alpha_0, \alpha_1, k) \in V_m^3. \tag{3}$$

Ясно, что ν_k — частичная раундовая функция сбалансированного алгоритма Фейстеля. Отметим, что условию (3) удовлетворяет алгоритм блочного шифрования GRANULE [10].

В данной работе для семейства l-раундовых сбалансированных алгоритмов шифрования Фейстеля с функцией усложнения, удовлетворяющей условиям (1)–(3), предложен способ построения невозможных разностей для произвольного числа раундов, а также приведена аналитическая оценка числа таких разностей. Метод не зависит ни от биективных компонент функции усложнения, ни от алгоритма развёртывания ключа. Основой его является следующая теорема:

Теорема 1. Пусть A — произвольная $(m \times m)$-матрица над полем $\mathrm{GF}(2)$, $\mathrm{rank}(A) = m-1$, раундовая функция $\nu : V_m^2 \times V_m \to V_m^2$ задана условием (3). Тогда для каждого натурального $l > 3$ у l-раундового алгоритма шифрования с раундовой функцией ν существует не менее $3 \times 2^{2n-2} - 2^{n+1}$ невозможных l-раундовых нетривиальных разностей.

Предложенный в [9] алгоритм поиска невозможных разностей не учитывает ключевую особенность алгоритма шифрования GRANULE, а именно необратимость функции усложнения. Произведена его модификация путём изменения способа зашифрования разностей на описанный в [11]. Это позволило улучшить результаты [9] относительно числа найденных 7-раундовых различителей, а также получить экспериментальное подтверждение справедливости теоремы 1.

ЛИТЕРАТУРА

1. *Biham E., Birukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials // J. Cryptology. 2005. V. 18. P. 12–23.
2. *Knudsen L. R.* DEAL — a 128-bit cipher // Complexity. 1998. V. 258(2). P. 216–224.
3. *Tezcan C.* Improbable differential attacks on Present using undisturbed bits // J. Comput. Appl. Math. 2014. V. 259. P. 503–511.
4. *Boura C., Naya-Plasencia M., and Suder V.* Scrutinizing and improving impossible differential attacks: Applications to CLEFIA, Camellia, LBlock and Simon // LNCS. 2014. V. 8873. P. 179–199.
5. *Phan R. C. W.* Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES) // Inform. Processing Lett. 2004. V. 91(1). P. 33–38.
6. *Li R., Sun B., and Li C.* Impossible differential cryptanalysis of SPN ciphers // IACR Cryptology ePrint Archive. 2010. V. 2010. P. 307–322.
7. *Wei Y., Li P., Sun B., and Li C.* Impossible differential cryptanalysis on Feistel ciphers with SP and SPS round functions // LNCS. 2010. V. 6123. P. 105–122.
8. *Cui T., Jin C., and Ma J.* A new method for finding impossible differentials of generalized Feistel structures // Chinese J. Electronics. 2018. No. 27(4). P. 728–733.
9. *Wu X., Li Y., Wei Y., and Sun Y.* Impossible differential distinguisher analysis of GRANULE and MANTRA algorithm // J. Communications. 2020. Iss. 1 P. 94–101.
10. *Bansod G., Pisharoty N., and Patil A.* GRANULE: An Ultra Lightweight Cipher Design for Embedded Security. IACR Cryptology ePrint Archive. 2018. `https://eprint.iacr.org/2018/600.pdf`.