УДК 519.7 DOI 10.17223/2226308X/11/22

ШИФР NSUPRESENT: УСТОЙЧИВОСТЬ К ЛИНЕЙНОМУ И ДИФФЕРЕНЦИАЛЬНОМУ КРИПТОАНАЛИЗАМ[1]

Е. А. Манылов

Рассмотрен шифр NSUPresent — модификация известного легковесного блочного шифра Present. Исследуется криптографическая стойкость данного шифра к линейному и дифференциальному криптоанализам. Получены теоретические оценки на дифференциальную и линейную характеристики шифра. Показано, что достаточно пяти раундов шифра NSUPresent, чтобы обеспечить устойчивость шифра к линейному и дифференциальному криптоанализам.

Ключевые слова: *легковесный блочный шифр, SP-сеть, линейный криптоанализ, дифференциальный криптоанализ.*

Пусть $\mathbb{F}_2^n$ — множество всех двоичных векторов длины n. *Весом Хэмминга* $\mathrm{wt}(x)$ двоичного вектора $x \in \mathbb{F}_2^n$ называется количество единиц, содержащихся в x. *Векторной булевой функцией* называется функция вида $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Функцию F также записывают как $F = (f_1, \ldots, f_m)$, где $f_1, \ldots, f_m$ — *координатные* булевы функции от n переменных, а функции $\langle b, F\rangle = b_1 f_1 \oplus b_2 f_2 \oplus \ldots \oplus b_m f_m$ называются *компонентными*, где $b \in \mathbb{F}_2^m$. *Спектром Уолша — Адамара* векторной функции F называется набор коэффициентов $W_{\langle b,F\rangle}(y) = \sum\limits_{x \in F_2^n} (-1)^{\langle b,F\rangle \oplus \langle x,y\rangle}$. Функцию $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ можно рассматривать как функцию над конечным полем $\mathbb{F}_{2^n}$ и однозначно представлять в виде полинома степени не выше $2^n - 1$: $F(x) = \sum\limits_{i=0}^{2^n-1} \delta_i x^i$, где $\delta_i \in \mathbb{F}_{2^n}$.

SP-сеть (подстановочно-перестановочная сеть) — одна из моделей построения итеративных блочных шифров — состоит из S-блоков, замещающих набор входных битов на соответствующий набор выходных битов, и P-блоков, перемешивающих биты. S-блок размера n — это отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ (как правило, взаимно однозначное).

Рассмотрим модификацию легковесного блочного шифра Present [1], в основе которого лежит SP-сеть (длина блока 64 бит, 31 раунд, слой S-блоков состоит из 16 одинаковых S-блоков размера 4). В отличие от Present, слой S-блоков NSUPresent состоит из четырёх S-блоков размера 16. Будем использовать перемешивающий слой шифра Present. Цель данной работы — найти минимальное количество раундов шифра NSUPresent, необходимое для криптографической стойкости шифра к линейному и дифференциальному криптоанализам.

Введем для вектора $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ следующие множества:

$$gr_I(a) = \{[(i-1)/4] + 1 : a_i = 1\}, \quad gr_O(a) = \{i \bmod 4 : a_i = 1\}.$$

Если a — входной вектор S-блока, то множество $gr_I(a)$ задаёт *активные входные группы* S-блока, если выходной, то множество $gr_O(a)$ задаёт *активные выходные группы* S-блока. Структура P-слоя такова, что каждая выходная группа S-блока связана ровно с одной входной группой S-блока следующего раунда.

Будем использовать S-блок $F : \mathbb{F}_2^{16} \to \mathbb{F}_2^{16}$ с дополнительными условиями:

1) для любой ненулевой входной разности $\delta^I \in \mathbb{F}_2^{16}$ и любой ненулевой выходной разности $\delta^O \in \mathbb{F}_2^{16}$ выполняется $|\{x \in \mathbb{F}_2^{16} : F(x) \oplus F(x \oplus \delta^I) = \delta^O\}| \leqslant 4$;

[1]Работа поддержана грантами РФФИ, проекты № 18-31-00479 и 18-07-01394.

2) для любой ненулевой входной разности $\delta^I \in \mathbb{F}_2^{16}$, такой, что $|gr_I(\delta^I)| = 1$, выходная разность $\delta^O = F(x) \oplus F(x \oplus \delta^I)$ такова, что $|gr_O(\delta^O)| \geqslant 2$;
3) для любого $a \in \mathbb{F}_2^{16}$ и всех ненулевых $b \in \mathbb{F}_2^{16}$ выполняется $|W_{\langle b,F\rangle}(a)| \leqslant 2^9$;
4) для всех $a \in \mathbb{F}_2^{16}$ и всех $b \in \mathbb{F}_2^{16}$, таких, что $|gr_I(a)| = 1$ и $|gr_O(b)| = 1$, выполняется $|W_{\langle b,F\rangle}(a)| \leqslant 2^8$.

Первое и второе условия определяют дифференциальную характеристику S-блока и позволяют увеличить количество активных S-блоков при проведении дифференциального криптоанализа; третье и четвёртое определяют линейную характеристику S-блока.

Отметим, что функция, удовлетворяющая данным условиям, существует, например функция обращения элемента в поле, используемая в шифре AES.

Утверждение 1. Существуют коэффициенты $a, b \in \mathbb{F}_{2^{16}}$, такие, что функция обращения $F(x) = ax^{-1} + b$ удовлетворяет условиям 1–4.

Основа *линейного криптоанализа* [2] — поиск линейного приближения, которое содержит биты открытого текста и шифртекста и имеет наибольшую вероятность выполнения. *Линейная характеристика* шифра — вероятность выполнения найденного линейного приближения.

Теорема 1. Линейная характеристика для пяти раундов шифра NSUPresent меньше чем 2^{-35}.

В основе *дифференциального криптоанализа* [3] лежит анализ пар открытых текстов (P, P') и соответствующих им пар шифртекстов (C, C'), между которыми существуют определённые разности, или дифференциалы $\alpha = P \oplus P'$, $\beta = C \oplus C'$. *Дифференциальная характеристика шифра* — максимальная вероятность выполнения пары (α_0, β_0) из всевозможных пар (α, β).

Теорема 2. Дифференциальная характеристика для пяти раундов шифра NSUPresent меньше чем 2^{-84}.

Для теорем 1 и 2 получены аналитические доказательства, в которых использованы свойства функции обращения и условия, накладываемые на S-блок.

Следствие 1. Для проведения успешной атаки с помощью линейного криптоанализа потребуется более 2^{70} пар открытых текстов / шифртекстов, а для дифференциального криптоанализа — более 2^{84} пар текстов.

Так как на вход шифра подаются блоки длины 64, то максимально возможное количество пар открытый текст / шифртекст равно 2^{64}. Следовательно, для проведения данных атак таких пар недостаточно.

ЛИТЕРАТУРА

1. *Bogdanov A., Knudsen L. R., Leander G., et al.* PRESENT: An ultra-lightweight block cipher // CHES 2007. LNCS. 2007. V. 4727. P. 450–466.
2. *Matsui M.* Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT'93. Berlin: Springer, 1994. P. 386–397.
3. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4. No. 1. P. 3–72.