УДК 519.7

М.А. ПУДОВКИНА, А.М. СМИРНОВ
Национальный исследовательский ядерный университет «МИФИ», Москва

ПРИМЕНЕНИЕ ПОДХОДА «ЙО-ЙО» ДЛЯ АТАКИ НА АЛГОРИТМ LILLIPUT-TBC-II-256

В работе обобщается подход «йо-йо» для атаки на произвольное число раундов алгоритма LILLIPUT-TBC-II-256 с ключом длины 256 бит. Для атаки требуется $2^{128} + 2^{16}$ текстов, $30 \cdot 2^{16}$ бит памяти. Трудоемкость атаки равна $31 \cdot (2^{128} + 2^{80})$ операций зашифрования. Вероятность успеха атаки равна 1.

В [1] предложена атака на 5-раундовый алгоритм блочного шифрования AES и описан для него 6-раундовый различитель, основанные на подходе из игры «йо-йо». Идея атаки состоит в использовании свойства XSL-алгоритмов блочного шифрования, включая обобщения SAS и SASAS [2], которое сохраняет нулевую разность между байтами векторов состояния. В данной работе, используя предложенную модификацию подхода «йо-йо», анализируется 32-раундовый алгоритм LILLIPUT-TBC-II-256 с длиной ключа 256 бит, участвующий в конкурсе американского института стандартизации (NIST) на стандарт низкоресурсного алгоритма шифрования США [2].

Пусть $V_{16}(2^8)$ – 16-мерное векторное пространство над полем $\mathbb{F}_{2^{32}}$; $\oplus -$ операция сложения в $V_{16}(2^8)$; $I(A)$ – индикатор выполнения условия A; $g: V_{16}(2^8) \times V_{16}(2^8) \longrightarrow V_{16}(2^8) -$ раундовая функция алгоритма LILLIPUT-TBC-II-256; $k \in V_{16}(2^8)$ – раундовый ключ; h – (0,1)-матрица порядка 16 над полем $\mathbb{F}_{2^8}$ линейного слоя раундовой функции g; s – фиксированная подстановка S-бокса; $\varepsilon_j -$ базисный вектор пространства $V_{16}(2^8)$, $j \in \{0, \dots, 15\}$, у которого j-я координата равна единице, а все остальные координаты нулевые.

Для каждых $\alpha = (\alpha_0, \dots, \alpha_{15}) \in V_{16}(2^8)$ и $k \in V_{16}(2^8)$ раундовая функция g задается условием

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

Для отображения $\chi^{(i)}: V_{16}(2^8) \longrightarrow \mathbb{F}_2$,

$$\chi^{(i)}(\alpha) = I(\alpha_i \neq 0), \qquad i = 0, \dots, 15,$$

положим $\chi(\alpha) = \left(\chi^{(0)}(\alpha), \dots, \chi^{(15)}(\alpha)\right)$.

Матрицу h представим в блочно-диагональном виде с (4×4)-подматрицами $h_{i,j}$, $i,j = 0,\dots,3$.

На основании следующих теорем 1, 2 разработана атака на полнораундовый алгоритм LILLIPUT-TBC-II-256, использующая модификацию подхода «йо-йо».

Теорема 1. *Пусть* $\alpha_0, \alpha_1, k_0, \dots, k_{30}$ – *произвольные элементы векторного пространства* $V_{16}(2^8)$, $\beta_i = g_{k_{30}} \dots g_{k_1} g_{k_0}(\alpha_i), i = 0,1$. *Тогда справедливо равенство*

$$\chi((sh)^{-2}(\beta_0) \oplus (sh)^{-2}(\beta_1)) = \chi(g_{k_{28}} \dots g_{k_0}(\alpha_0) \oplus g_{k_{28}} \dots g_{k_0}(\alpha_1)).$$

Теорема 2. *Пусть* $\alpha, k \in V_{16}(2^8)$ *и существуют такие* $i, j_1, j_2 \in \{0, \dots, 15\}$, *что элементы матрицы линейного отображения* h^{-1} *удовлетворяют условиям*

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

Тогда для каждого $\omega \in \mathbb{F}_{2^8}$ *существует такое* $\delta \in \mathbb{F}_{2^8}$, *что уравнение*

$$((sh)^{-1}(\alpha \oplus \omega \cdot \varepsilon_{j_2} \oplus k) \oplus (sh)^{-1}(\alpha \oplus \delta \cdot \varepsilon_{j_1} \oplus (\delta \oplus \omega) \cdot \varepsilon_{j_2} \oplus k))_i = 0$$

имеет 2^8 *решений.*

Доказано, что для атаки требуется $2^{128} + 2^{16}$ текстов, $30 \cdot 2^{16}$ бит памяти, а трудоемкость атаки составляет $31 \cdot (2^{128} + 2^{80})$ операций зашифрования. Вероятность успеха атаки равна 1

Список литературы

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

2. Biryukov A., Shamir A. Structural cryptanalysis of SASAS // EUROCRYPT'01, Lect. Notes Comput. Sci. 2001. V. 2045. P. 394–405.

3. Adomnicai A., Berger T. P., Clavier C., Francq J., Huynh P., Lallemand V., GouguecK.Le, MinierM., ReynaudL. and ThomasG. Lilliput-AE: a New Lightweight Tweakable Block Cipher for Authenticated Encryption with Associated Data // NIST Lightweight Cryptography Standardization Process, 2019. https://csrc.nist.gov/Projects/Lightweight-Cryptography.