

# ПЕРЕВІРКА СТАТИСТИЧНИХ ВЛАСТИВОСТЕЙ ВИПАДКОВИХ S-БЛОКІВ ВІДНОСНО ОПЕРАЦІЇ ДОДАВАННЯ ЗА МОДУЛЕМ $2^n$

М. П. Оксьоненко<sup>1</sup>

<sup>1</sup>Національний технічний університет України «Київський політехнічний інститут»

## Анотація

Перевірено статистичні властивості S-блоків шифру ДСТУ-7624:214 «Калина» та його попередньої версії 2007-го року щодо розподілу коефіцієнтів таблиці ймовірностей диференціалів за операцією додавання за модулем  $2^n$ .

**Ключові слова:** S-блок, таблиця ймовірностей диференціалів, розподіл Пуассона

## Вступ

У 2015 році в Україні був прийнятий новий національний стандарт блокового шифрування ДСТУ 7624:2004 («Калина») [1]. В даній роботі будуть перевірені властивості розподілу коефіцієнтів таблиці ймовірностей диференціалів за операцією додавання за модулем  $2^n$ .

## 1. Необхідні терміни та позначення

S-блок – функція, що приймає на вхід  $n$  біт і перетворює їх за визначеним правилом, видаючи на виході  $m$  біт.  $n$  та  $m$  не обов'язково рівні між собою. Якщо  $m = n$ , то мова йде про бієктивний S-блок. В шифрах, які ми розглядаємо, використовуються саме бієктивні перетворення.

Нехай  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  – деяке відображення. *Таблиця ймовірностей диференціалів* (Difference Distribution Table, DDT) відображення  $f$  – матриця  $\|d_{ij}\|$  розмірності  $2^n \times 2^n$ , де кожний елемент  $d_{ij}$  знаходиться за формулою:

$$d_{ij} = |\{x \in \{0, 1\}^n : f(x \oplus i) \oplus f(x) = j\}|$$

Ймовірності диференціалів визначають стійкість криптоперетворень до диференціального криптоаналізу.

## 2. Розподіл модифікованої DDT на S-блоках

Як було показано в [1], коефіцієнти в DDT, операцією  $\oplus$  має розподіл Пуассона з параметром  $1/2$ . Якщо розглядати таблицю ймовірностей диференціалів з операцією додавання за модулем  $2^n$ , то дані коефіцієнти мають розподіл Пуассона з параметром 1. Тому можемо побудувати теоретичну оцінку для нового розподілу й перевірити практичні значення на S-блоках «Калини». Визначимо теоретичну ймовірність, що для випадкового S-блоку максимальне

значення  $\lambda$  таблиці DDT з операцією додавання за модулем  $2^n$  буде зустрічатись  $N$  разів.

Для DDT 8-бітного S-блоку відповідна ймовірність оцінюється за формулою:

$$Pr(\lambda, N) = \sum_{l=0}^N \left( \binom{l}{255^2} \cdot \left[ \sum_{d=0}^{\lambda-1} D(d) \right] \cdot D(\lambda)^l \right),$$

де  $D(d) = e^{-1}/d!$  – ймовірність розподілу Пуассона з параметром 1.

Було розглянуто 8 S-блоків  $S_0, \dots, S_7$  з шифру «Калина» 2007 р. [1] та чотири S-блоки  $\pi_0, \dots, \pi_3$  з шифру «Калина» 2014 р [1] і побудовані таблиці DDT за операцією додавання за модулем  $2^n$  і обчислено значення параметрів  $\lambda$ ,  $N$ ,  $Pr(\lambda, N)$ .

Автори «Калини» стверджували, що S-блоки були обрані випадковим чином, що й було метою перевірити. S-блоки, які мають подібні характеристики, досить легко згенерувати випадковим чином.

## Висновки

Була проведена модифікація таблиці ймовірностей диференціалів, яка заснована на переході від операції  $\oplus$  до операції додавання за модулем  $2^n$ . Розподіл коефіцієнтів в модифікованій DDT S-блоків «Калини» показав можливість випадкової генерації таких перестановок за допомогою невеликої кількості обчислювальних ресурсів, що не суперечить твердженню авторів про те, що S-блоки були знайдені шляхом випадкового пошуку.

## Перелік використаних джерел

1. R. Oliynykov, I. Gorbenko, O. Kazymyrov, V. Ruzhentsev, O. Kuznetsov, Y. Gorbenko, O. Dyrda, V. Dolgov, A. Pushkaryov, R. Mordvinov, D. Kaidalov. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. – 2015