УДК 003.26:519.21

МАТРИЦЯ ІНДИКАТОРІВ НАЙБІЛЬШИХ СТЕПЕНІВ ДЛЯ ФЕЙСТЕЛЬ-ПОДІБНИХ ПЕРЕТВОРЕНЬ

Оксьоненко Максим, Яковлєв Сергій

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут

Анотація

У роботі проводиться уточнення методів виявлення прихованих аналітичних структур, зокрема, фейстель-подібних перетворень, за допомогою матриці індикаторів найбільших степенів. Показано, який вигляд має матриця індикаторів найбільших степенів для схеми MISTY та R-схеми в залежності від кількості раундів та алгебраїчного степеня раундової функції.

Abstract

In this paper we clarify a method for hidden analytical structures detection in Feistel-like networks, based on High-Degree Indicator matrix. We find a form of High-Degree Indicator matrix depending on number of rounds and algebraic degree of round function for both MISTY and R-scheme.

Вступ

Одним із найпоширеніших методів криптографічного захисту конфіденційності інформації є блочні симетричні шифри. Питання про їхню стійкість турбує криптографічну спільноту й є як ніколи актуальним. Зараз для побудови блокових шифрів часто використовують мережі Фейстеля. Вони набули популярності через те, що можуть бути легко реалізовані як апаратно, так і програмно й мають гарні криптографічні властивості. У зв'язку з такою популярністю з'явилось багато варіантів фейстель-подібних мереж, таких, як схема MISTY або R-схема, які можуть відрізнятися складністю реалізації та криптографічними властивостями.

Стійкість більшості сучасних блокових шифрів ґрунтується на S-блоках – складних нелінійниз перетворення. У останні роки для протидії алгебраїчним методам криптоаналізу такі S-блоки генерують випадковим чином, однак це не гарантує, що така випадково згенерована перестановка не містить внутрішніх струкутур, які призводять до зменшення стійкості шифру до певного класу атак. Знайдено методи, які дозволяють розпізнавати звичайні фейстелівські перетворення на основі обчислення для них матриць індикаторів найвищих степенів [1]. У даній роботі дані методи поширюються та узагальнюються для схеми MISTY та R-схеми.

Матриця індикаторів найбільших степенів

Виявлення прихованих фейстель-подібних структур проводиться на основі виду матриці індикаторів найбільших степенів (*High-Degree Indicator matrix, HDIM*). Якщо маємо n-бітову перестановку *F*, то її матриця індикаторів найбільших степенів має вид:

$$H(F)[i,j] = \bigoplus_{x \in F_2^n} (e_i \cdot F(x))(e_j \cdot x)$$

Коефіцієнти матриці *H(F)* показують присутність найвищого степеня в алгебраїчній нормальній формі координатних функцій *F*. Максимальна степінь *d* схеми Фейстеля й кількість раундів *r* корелюють з виглядом матриці індикаторів найбільших степенів.

Один раунд кожної фейстель-подібної схеми використовує деяке внутрішнє перетворення $f : V_n \to V_n$; при цьому на різних раундах можуть використовуватись різні

перетворення. Раундові функції схеми, які далі будуть розглядатись, мають таке представлення у наведеній вище формі.

1. Схема MISTY: $F(x, y) = (y, y \oplus f(x))$
2. R-схема: $F(x, y) = (y \oplus f(x), f(x))$

Поведінка HDIM для схеми MISTY та R-схеми описується у наступних теоремах.

Теорема 1:

Нехай *F* – *2n*-бітова *r*-раундова схема MISTY з раундовими функціями f_k, і нехай $\deg(f_k) \le d$, $\deg(f_k^{-1}) \le D$. Тоді $H(F)[i, j] = 0$, якщо:

1. $i < n$:
   a. $r = 4l + 3$ та $\theta = d^{l+1} + D^{2l+1} < 2n$,
   b. $r = 4l + 2$ та $\theta = d^{l+1} + D^{2l} < 2n$,
   c. $r = 4l + 1$ та $\theta = d^{l} + D^{2l} < 2n$,
   d. $r = 4l$ та $\theta = d^{l} + D^{2l-1} < 2n$;
2. $n \le i < 2n$:
   a. $r = 4l + 3$ та $\theta = d^{l} + D^{2l+1} < 2n$,
   b. $r = 4l + 2$ та $\theta = d^{l} + D^{2l} < 2n$,
   c. $r = 4l + 1$ та $\theta = d^{l} + D^{2l} < 2n$,
   d. $r = 4l$ та $\theta = d^{l} + D^{2l-1} < 2n$.

Теорема 2:

Нехай *F* – *2n*-бітова *r*-раундова R-схема з раундовими функціями f_k, і нехай $\deg(f_k) \le d$, $\deg(f_k^{-1}) \le D$. Тоді $H(F)[i, j] = 0$ для будь-якого *i* та *j*, якщо:

1. $r = 4l + 3$ та $\theta = d^{2l+1} + D^{l+1} < 2n$,
2. $r = 4l + 2$ та $\theta = d^{2l+1} + D^{l} < 2n$,
3. $r = 4l + 1$ та $\theta = d^{2l} + D^{l} < 2n$,
4. $r = 4l$ та $\theta = d^{2l} + D^{2l} < 2n$.

З теореми випливає, що для R-схеми, при невеликих значеннях параметрів *d* та *r* матриця індикаторів найбільших степенів повністю заповнена нулями. Аналогічно приведені випадки для схеми MISTY, але нульовою буде не вся матриця, а тільки ліва або права половина що відрізняється від вигляду матриці для класичної схеми Фейстеля, в якій або три квадранти матриці (окрім нижнього правого), або один лівий верхній квадрант будуть повністю нульовими. Отже деякі фейстель-подібні перетворення можуть бути ідентифіковані за допомогою облислення матриці індикаторів найбільших степенів.

Список використаних джерел

1. Leo Perrin, Aleksei Udovenko. Algebraic Insights into the Secret Feistel Network [Електронний ресурс] / Perrin L., Udovenko A. – 2016. – Режим доступу до ресурсу: https://eprint.iacr.org/2016/398.pdf