УДК 004.056.55:519.2

РОЗПІЗНАВАННЯ ПРИХОВАНИХ MISTY-ПОДІБНИХ ПЕРЕТВОРЕНЬ

Оксьоненко Максим, Яковлєв Серій

Фізико-технічний інститут, КПІ ім. Ігоря Сікорського

Анотація

В роботі розглянуто новий запропонований підхід до виявлення прихованих структур у таблично заданих S-блоках, який використовує так звану індикаторну матрицю високого порядку (HDIM-матрицю). Показано, що S-блоки, побудовані на основі схеми MISTY, при певних обмеженнях на кількість раундів та степінь раундової функції мають чіткі шаблони у HDIM-матриці, що може бути виявлено під час незалежного відновлення внутрішньої структури.

Abstract

We considered new proposed method for hidden structure detection in tabular S-boxes, which uses so-called High-Degree Indicator Matrix (HDIM). We show that S-boxes based on the MISTY scheme have strong patterns under certain restrictions, what can be detected during recovering of the internal structure.

Вступ

У роботі [2] запропонували метод визначення прихованої структури схеми Фейстеля у S-блоках за допомогою аналізу так званої HDIM-матриці. Зокрема, виявилось, що при деяких обмеженнях на степінь раундової функції схеми Фейстеля та кількість раундів, великі фрагменти HDIM-матриці залишаються нульовими. Схема блокового шифрування MISTY [3] є аналогом схеми Фейстеля, яка, втім, може більш ефективно обчислюватись за рахунок паралелізації обчислень сусідніх раундів, що є привабливою властивістю для ефективних реалізацій алгоритмів шифрування у малопотужних пристроях. У даній роботі наводяться знайдені особливості HDIM-матриць схем MISTY, що також дозволяє шукати приховані структури у таблично заданих S-блоках.

Необхідні терміни та визначення

Введемо необхідні для викладення результатів терміни та поняття [1].

Нехай $F_2 = \{0,1\}$, $F_2^n = \{0,1\}^n$. Одновимірна булева функція – це довільне відображення з множини F_2^n в множину F_2. Багатовимірна (векторна) булева функція – довільне відображення з F_2^n у F_2^m. Кожна *m*-вимірна булева функція *F* може бути представлена у вигляді вектору одновимірних координатних функцій: $F = (f_0,..., f_{m-1})$.

Позначимо також через e_i двійковий вектор, у якого *i*-та координата дорівнює 1, а всі інші – нульові.

Кожна булева функція може бути однозначно представлена канонічним поліномом над F_2 у вигляді так званої алгебраїчної нормально форми (АНФ). Алгебраїчна степінь $\deg(f)$ булевої функції f дорівнює найбільшій кількості змінних у термах її АНФ. Степінь багатовимірної функції дорівнює максимальній степені її координатних функцій.

Нехай *F* – *n*-вимірна булева функція від *n* змінних. *Індикаторна матриця високих порядків* функції *F*, або просто *HDIM-матриця* (High-Degree Indicator matrix, HDIM [2]) $\hat{H}(F)$ – двійкова матриця розмірності $n \times n$, елементи якої визначаються як

$$\hat{H}(F)[i, j] = \bigoplus_x (e_i \cdot F(x)) \cdot (e_j \cdot x) = \bigoplus_x (e_j \cdot x) \cdot f_i(x) \cdot .$$

Коефіцієнти матриці $\hat{H}(F)$ показують присутність доданку степеня $n-1$, який не містить змінної x_j, в АНФ координатної функції f_i.

Схема MISTY – ітеративна схема блокового шифрування, яка перетворює блоки довжини $2n$ у блоки довжини $2n$, один раунд шифрування якої має вид $F_k(x,y)=(y, y\oplus f_k(x))$, де $x,y\in F_2^n$, f – бієктивна раундова функція. Для побудови S-блоків використовуються схеми блокового шифрування малого розміру з константно заданими ключами (наприклад, нульовими).

Розпізнавання прихованих MISTY-подібних перетворень

Нехай E $2n$-бітова схема MISTY ($n>2$) із непарною кількістю раундів і раундовою функцією f, причому $\deg(f)=d$, $\deg(f^{-1})=\tilde{d}$. Одержані результати подамо у вигляді двох таких теорем.

Теорема 1. За виконання таких умов:

1) при $r=4l+3$: $d^{l+1}+\tilde{d}^{2l+1}<2n$;

2) при $r=4l+1$: $d^{l}+\tilde{d}^{2l}<2n$;

завжди маємо $\hat{H}(F)[i,j]=0$ при довільному $0\le i<n$ та довільному j.

Теорема 2. За виконання таких умов:

1) при $r=4l+3$: $d^{l}+\tilde{d}^{2l+1}<2n$;

2) при $r=4l+1$: $d^{l}+\tilde{d}^{2l}<2n$;

завжди маємо $\hat{H}(F)[i,j]=0$ при довільному $i\ge n$ та довільному j.

З теорем випливає, що уся ліва або уся права частина HDIM-матриці буде заповнена нулями при виконанні зазначених умов. Таким чином, при невеликій кількості раундів (та виконання умов) уся HDIM-матриця схеми MISTY є нульовою. При більшій кількості раундів гарантовано занулюватись може лише права половина; при порушенні наведених умов поведінка елементів HDIM-матриці невідома. Одержані результати узагальнюються на парну кількість раундів (але із більш складними умовами)

Отже, одержані результати дозволяють на перших кроках аналізу визначати, чи має таблично заданий S-блок приховану структуру MISTY-подібного перетворення.

Висновки

У даній роботі розглянуто нещодавно запропонований метод виявлення прихованих структур у таблично заданих S-блоках за допомогою так званої індикаторної матриці високих порядків (HDIM-матриці). Показано, що перетворення зі структурою схеми MISTY мають певні особливості у HDIM-матриці, які можуть бути виявлені. Сформульовано умови, за яких зазначені особливості мають місце. Порушення цих умов при побудові S-блоку дозволяє захистись від даного методу аналізу.

Список використаних джерел:

1.C. Carlet. Boolean functions for cryptography and error correcting codes [електронний ресурс]. – 2006. – Режим доступу:
http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf

2.L. Perrin, A. Udovenko. Algebraic Insights into the Secret Feistel Network (Full Version) [електронний ресурс]. – 2016. – Режим доступу: http://eprint.iacr.org/2016/398.

3.Matsui M. On a Structure of Block Ciphers with Provable Security against Differential and Linear Analysis // IEICE Trans. Fundamentals. – Vol. E82-A. – #1. – 1999. – pp. 117-122.