СТІЙКІСТЬ SPARX-64/128 ДО ДИФЕРЕНЦІЙНИХ АТАК

Іщук О. Р., Руженцев В. І.
Харківський національний університет радіоелектроніки, Харків, Україна

Диференційний криптоаналіз – це статистична атака на симетричне криптоперетворення, яка вивчає зміну різниці між двома парами тестів по мірі їх проходження через компоненти перетворення. Така різниця може бути використана для призначення ймовірностей можливим ключам і навіть для визначення найбільш ймовірного серед них.

SPARX-64/128 – це базований на ARX(add, rotation, xor) перетвореннях блочний шифр, де 64 бітний блок тексту і 128 бітний ключ. Він був опублікований в 2016 році на міжнародній конференції Asiacrypt 2016 [1].

Проблема через яку з'явився цей шифр звучить так «Чи можливо створити ARX шифр який буде захищений від диференційних та лінійних криптоатак».

Шифр SPARX ефективний з точки зору пам'яті, розміру коду та часу. Завдяки використанню операцій ARX, він за своєю суттю більш захищений від атак з боку бічних каналів, ніж шифр на основі S-Box, як-от AES. Крім того, на відміну від усіх інших ARX, які мають ці переваги, шифри SPARX є єдиними блочними шифрами на основі ARX, для яких можна довести межі ймовірності диференціальних та лінійних слідів. Це означає, що безпеку, яку він забезпечує, легше виправдати, ніж для інших подібних шифрів. Структура SPARX також допускає функціонально еквівалентні реалізації з різними властивостями.

Наприклад, підключі можуть бути отримані на льоту, щоб зменшити обсяг пам'яті, або попередньо обчислені, щоб скоротити час обчислень.

Мета роботи - дослідження стійкісты шифру SPARX-64/128 до диференційних атак.

Для досягнення цілі на першому етапі потрібно вирішити наступні завдання: розробити програмну реалізацію алгоритму шифрування з можливістю зміни кількості циклів, перевірити наявність нездійснених диференціалів, тобто необхідну умову організації відповідної атаки. Результати виконання цих завдань представлені у доповіді.

Список літератури

1. Daniel Dinu, L´eo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschadl,and Alex Biryukov. Design Strategies for ARX with Provable Bounds: Sparx and LAX. In Jung Hee Cheon and Tsuyoshi Takagi, editors, Advances in Cryptology – ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I, pages 484–513. Springer Berlin Heidelberg, 2016.