**УДК 004.056.55**
**О. Ярема**
Тернопільський національний технічний університет імені Івана Пулюя, Україна

# ПРАКТИЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ СТІЙКОСТІ S-БЛОКІВ ДО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ

**O. Yarema**

# PRACTICAL ASPECTS OF RESEARCH ON THE RESISTANCE OF S-BLOCKS TO DIFFERENTIAL CRYPTANALYSIS

S-блоки (блоки підстановки) є ключовим елементом багатьох блокових шифрів, таких як DES та AES. Вони використовуються для забезпечення нелінійності в процесі шифрування, що є критично важливим для забезпечення стійкості шифру до різних видів криптоаналітичних атак, як статистичних, так і алгебраїчних. S-блоки є статичними для конкретної реалізації блокового шифру з деякими винятками [1] і не залежать від секретного ключа, що робить їх одним з головних об'єктів атаки на шифр. S-блоки можуть задаватися таблично (див. рисунок 1) або як набір інструкцій алгебраїчних перетворень для вхідних бітів.

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 |
|---|---|---|---|---|---|---|---|---|---|
| **00** | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 |
| **10** | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad |
| **20** | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 |
| **30** | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 |
| **40** | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 |
| **50** | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a |
| **60** | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 |
| **70** | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc |
| **80** | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 |

Рисунок 1. Частина табличного задання S-блока шифру AES

Визначення, чи підходить конкретний S-блок для використання в шифрі, відбувається на основі дослідження основних криптографічних властивостей S-блоків: критерію лавини, нелінійності, незалежності бітів, диференційної рівномірності, зворотності та несуперечності.

Критерій лавини є мірою того, наскільки ефективно S-блок розповсюджує вхідні зміни на вихідні біти. Якщо зміна одного біту на вході призводить до зміни багатьох бітів на виході, то критерій лавини вважається виконаним [2]. Більш стійкою характеристикою блоків підстановки є строгий критерій лавини.

Нелінійність S-блоку забезпечує, що висока лінійна кореляція між вхідними та вихідними бітами буде мінімальною, що робить лінійний криптоаналіз менш ефективним [3].

Незалежність бітів означає, що зміна одного біту вхідної інформації не повинна мати вплив на інші біти вихідної інформації. Ця властивість демонструє, що кожен біт вихідної інформації може бути обчислений незалежно від інших. По суті, ця властивість характеризує те ж явище, що й критерій лавини, але з іншої точки зору [4].

Диференційна рівномірність вказує на те, як часто можливий певний диференціал між двома блоками даних. Чим менше ймовірність того, що можливий диференціал зустріне, тим більша стійкість шифру до диференціальних атак.

Зворотність та несуперечність це пов’язана пара властивостей, які описують те, чи для кожного вхідного значення існує лише одне відповідне вихідне значення і навпаки.

**Література**


1. Agarwal P., Singh A., Kilicman A. Development of key-dependent dynamic S-Boxes with dynamic irreducible polynomial and affine constant. Advances in mechanical engineering. 2018. Т. 10, № 7. С. 168781401878163. URL: https://doi.org/10.1177/1687814018781638 (дата звернення: 25.11.2023).
2. Kim K., Matsumoto T., Imai H. A recursive construction method of s-boxes satisfying strict avalanche criterion. Advances in Cryptology-CRYPT0’ 90. Berlin, Heidelberg. С. 565–574. URL: https://doi.org/10.1007/3-540-38424-3_39 (дата звернення: 25.11.2023).
3. Nyberg K. S-boxes and round functions with controllable linearity and differential uniformity. Fast software encryption. Berlin, Heidelberg, 1995. С. 111–130. URL: https://doi.org/10.1007/3-540-60590-8_9 (дата звернення: 25.11.2023).
4. Sinha S., Arya C. Algebraic construction and cryptographic properties of rijndael substitution box. Defence science journal. 2012. Т. 62, № 1. С. 32–37. URL: https://doi.org/10.14429/dsj.62.1439 (дата звернення: 25.11.2023).