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

ЕВРИСТИЧНІ МЕТОДИ ГЕНЕРАЦІЇ S-БЛОКІВ ТА ЇХ ПРОГРАМНА РЕАЛІЗАЦІЯ

UDC 004.056.55
O. Yarema

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

S-блоки (блоки підстановки), як один з елементів симетричних блокових шифрів, є основним методом забезпечення нелінійності шифрів. Існують багато способів генерації S-блоків, але в загальному всі вони входять до одної з трьох категорій: евристичні, алгебраїчні та комбіновані методи [1].

Евристичні методи є найпростішими та найбільш поширеними за рахунок своєї простоти. Ці методи використовують псевдовипадковості для генерації S-блоків, які потім перевіряються на відповідність заданим критеріям стійкості. За рахунок використання псевдовипадковостей такий спосіб просто реалізувати програмно і використовувати його для генерації великої кількості блоків. Проте евристичні методи не гарантують криптографічної стійкості і сильно залежать від того, які саме критерії оцінки стійкості обрані в конкретній реалізації [2].

Алгебраїчні методи використовують теорію груп, полів та інших алгебраїчних структур для генерації блоків. Такі блоки можуть мати високу криптографічну стійкість за рахунок використання доведених математичних властивостей. Недоліком таких методів є їх складність в реалізації та потреба в великих обчислювальних ресурсах.

Комбіновані методи, як очевидно з назви, комбінують підходи обох попередніх типів в певних пропорціях і дозволяють отримати дещо середні результати – блоки з непоганою криптографічною стійкістю та відносно простою реалізацією алгоритму генерації.

Варто окремо зауважити, що евристичні методи мають набагато вищу популярність серед шифрів, які використовують динамічні S-блоки [3], які генеруються на основі ключа. Таким шифрам зазвичай не підходять алгебраїчні методи через необхідність в швидкодії [4], що не притаманна алгебраїчним методам генерації S-блоків.

Література

1. Menezes A. J., van Oorschot P. C., Vanstone S. A. Overview of cryptography. Handbook of applied cryptography. 2018. С. 1–48. URL: https://doi.org/10.1201/9780429466335-1 (дата звернення: 01.12.2024).
2. Cryptanalytic attacks on IDEA block cipher / H. K. Sahu та ін. Defence science journal. 2016. Т. 66, № 6. С. 582. URL: https://doi.org/10.14429/dsj.66.10798 (дата звернення: 01.12.2024).
3. 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: 25.11.2024).
4. Sharma S., Patel K. N., Siddhath Jha A. Cryptography using blowfish algorithm. 2021 3rd international conference on advances in computing, communication control and networking (ICAC3N), м. Greater Noida, India, 17–18 груд. 2021 р. 2021. URL: https://doi.org/10.1109/icac3n53548.2021.9725661 (дата звернення: 01.12.2024).