УДК 681.3.06:006.354

ГЕНЕРАЦІЯ S-БЛОКІВ З ПОКРАЩЕНИМИ КРИПТОГРАФІЧНИМИ ВЛАСТИВОСТЯМИ

[*]**М.Ю. Родінко,** [**]**Р.В. Олійников**, д-р техн. наук, доц.;
[***]**О.В.Казимиров**, канд. техн. наук
[*]Харківський національний університет радіоелектроніки
e-mail: m.rodinko@gmail.com
[**]Приватне акціонерне товариство «Інститут інформаційних технологій»
[***]EVRY Norge AS

Застосування підстановок з оптимальними криптографічними показниками дозволяє поліпшити характеристики симетричних перетворень, що дає можливість зменшити число ітерацій алгоритму. Однак генерація оптимальних S-блоків є обчислювально складною задачею, що є неприйнятним, наприклад, при використанні S-блоків в якості ключових елементів. Таким чином, актуальною є задача оптимізації методів генерації S-блоків.

До сучасних критеріїв відбору S-блоків [1-3] відносяться: максимум в таблиці розподілу диференціальних різниць, максимум в таблиці лінійних апроксимацій, алгебраїчний імунітет, мінімальна степінь S-блока та відсутність нерухомих точок.

Метод пошуку S-блоків, що розглядається, в загальному випадку складається з двох етапів: генерації псевдовипадкової підстановки та її перевірки на відповідність заявленим критеріям.

Для генерації підстановок був обраний алгоритм [2], який передбачає формування перестановки на основі векторної булевої функції $F(x) = x^{-1}$ та подальший обмін місцями N значень перестановки.

Критерії відбору підстановок є частково взаємозалежними, тому змінюючи порядок їх застосування в ході перевірки підстановки можна істотно скоротити час розрахунків.

Нехай задано m критеріїв відбору підстановок. Тоді число можливих комбінацій m критеріїв, які задають порядок їх застосування, дорівнює $m!$.

Нехай σ – множина усіх таких комбінацій, а $\sigma_i \in \{0 \dots (m-1)!\}$ – i-а комбінація критеріїв наступного виду:

$$\sigma_i = \Phi_{m-1} \circ \Phi_{m-2} \circ \dots \circ \Phi_j \circ \dots \circ \Phi_0, \quad (1)$$

де Φ_j – j-ий критерій відбору у цій комбінації.

Введемо деяку функцію $T(\sigma_i)$, значення якої представляє собою час генерації однієї підстановки, що задовольняє усім m критеріям, із використанням комбінації критеріїв σ_i. Тоді задача мінімізації часу перевірки підстановки на відповідність m критеріям зводиться до знаходження t_{min}:

$$t_{min} = inf\ \{T(\sigma_i) \mid i = 0 \dots (m-1)!\}. \quad (2)$$

У ході експериментальних досліджень для підстановок степеня $n = 2^8$ були визначені наступні фактори, що впливають на час генерації підстановки:

- p_{Φ_j} – процент підстановок, що задовольняють критерію Φ_j;
- t_{Φ_j} – час перевірки однієї підстановки на відповідність критерію Φ_j.

Використовуючи введені фактори, отримуємо наступне співвідношення для знаходження $T(\sigma_i)$:

$$T(\sigma_i) = \sum_{j=0}^{m-1} (\theta_{\Phi_j} \cdot t_{\Phi_j}), \quad (3)$$

де $\theta_{\Phi_j} = (\theta_{\Phi_{j-1}} \cdot p_{\Phi_j})/100,\ \theta_{\Phi_{-1}} = 100.$

Нижче наведено приклад застосування цього підходу для генерації підстановок за чотирма наступними критеріями ($m = 4$):

1. δ – максимум таблиці диференціалів, що дорівнює 8.
2. λ – абсолютний максимум таблиці лінійних апроксимацій, що дорівнює 26.
3. μ – мінімальна степінь булевої функції, що дорівнює 7.
4. τ – алгебраїчний імунітет, що дорівнює 3.

Таким чином, потужність множини комбінацій критеріїв $|\sigma| = 24$.

Експериментальні значення, отримані для факторів p і t для чотирьох критеріїв, представлені в табл. 1.

Далі за формулою (3) були розраховані значення функції T для комбінацій критеріїв $\sigma_i \in \{0 \dots 23\}$ і знайдено мінімальне значення $t_{min} = 0{,}0540755$ при $\sigma_{22} = \tau \circ \mu \circ \delta \circ \lambda$.

Табл. 1. – Значення факторів для чотирьох критеріїв

Критерій	Фактор p, %	Фактор t, сек
δ	70	0,000169
λ	14	0,001655
μ	99,6	0,000016
τ	44,5	0,006698

Паралельно були отримані експериментальні значення часу перевірки підстановок $T_{експер}$ для усіх комбінацій критеріїв.

На рис. 1 представлені графіки функцій T (суцільна крива) и $T_{експер}$ (пунктирна крива).

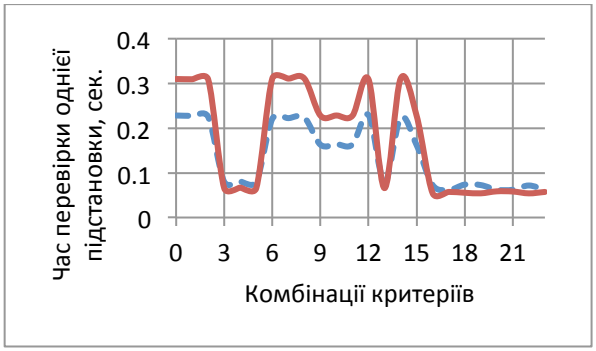

Рис. 1. – Графіки функцій T и $T_{експер}$

Представлений метод дозволив згенерувати оптимальні підстановки, що мають нелінійність 104 та описуються перевизначеною системою рівнянь 3-ої степені на персональній ЕОМ без використання розподілених обчислень.

Таким чином, запропоновано підхід до оптимізації методу генерації S-блоків, заснований на мінімізації часу перевірки підстановки на відповідність набору критеріїв. Експерименти показали, що при застосуванні оптимального порядку критеріїв час перевірки S-блоків зменшується приблизно в 5 разів.

Література

1. ***Олейников Р.В.*** Выбор S-блоков для симметричных криптографических алгоритмов на основе анализа алгебраических свойств / Р.В. Олейников, А. В. Казимиров // Вісн. Харк. нац. ун-ту. Сер. Математичне моделювання. Інформаційні технології. Автоматизовані системи управління. − Х., 2010. – № 925. – С. 79–86.
2. ***Казимиров О.В.*** Методи та засоби генерації нелінійних вузлів заміни для симетричних крипто алгоритмів / О.В. Казимиров // Дисертація на здобуття наукового ступеня кандидата технічних наук по спеціальності 05.13.21 – системи захисту інформації. ХНУРЕ. – Харків. – 2014.
3. ***Nyberg K.*** “Provable” security against differential and linear cryptanalysis / K. Nyberg // Fast Software Encryption. – V. 7549. – 2012. – pp. 1-8.

М.Ю. Родінко, Р.В. Олійников, О.В. Казимиров. **Генерація S-блоків з покращеними криптографічними властивостями.**

У доповіді представлений оптимізований метод генерації S-блоків, заснований на мінімізації часу перевірки підстановок на відповідність множині критеріїв. Запропонований метод дозволяє підвищити швидкість генерації підстановок у декілька разів та отримати оптимальні підстановки без застосування розподілених обчислень.

Ключові слова: *S-блок, криптоаналіз, таблиця розподілу різниць, таблиця лінійних апроксимацій, алгебраїчний імунітет.*

M.Yu. Rodinko, R.V. Oliynykov, O.V. Kazymyrov. **Generation of S-boxes with improved cryptographic properties.**

It is presented an optimized method of generation of S-boxes based on minimizing time of testing substitutions on the corresponding set of criteria. The optimized method allows speeding up the generation of substitutions up to several times and getting optimal substitutions without using distributed calculations.

Key words: *S-box, cryptanalysis, distribution table of differences, linear approximation table, algebraic immunity*.