УДК 681.3.06

О.М. БЕВЗ

ОБЧИСЛЮВАЛЬНІ ХАРАКТЕРИСТИКИ ПІДСТАНОВОЧНО-ПЕРЕСТАНОВОЧНИХ МЕРЕЖ З S-БОКСАМИ РОЗМІРОМ 16Х16 БІТ

Вінницький національний технічний університет
Хмельницьке шосе 95, м. Вінниця, 21021, Україна,
E-mail: ezorf@mail.ru

Анотація. В цій статті розглянута реалізація блочного шифру, який оснований на архітектурі гніздової постановочно-перестановочной сети (nested SPN), с блоками підстановки (S-боксами) розміром 16х16 біт в комп`ютерних системах. Визначено кількість табличних підстановок і розмір пам`яті для виконання двох послідовних рівнів гніздових підстановочно-перестановочних мереж різного типу.

Аннотация. В данной статье рассматривается реализация блочного шифра, основаного на архитектуре гнездовой постановочно-перестановочной сети (nested SPN), с блоками подстановки (S-боксами) размером 16х16 бит в компьютерных системах. Определены число табличных подстановок и размер необходимой памяти для выполнения двух последовательных уровней гнездовых подстановочно-перестановочных сетей разного типа.

Abstract. This note contains a realization of block cipher in computing system. This cipher use a nested substitution-permutation networks as architecture. The size of S-box is 16x16 bites. A number of table substitution and a size of memory for two levels nested substitution-permutation networks are defined too.

Ключові слова: підстановочно-перестановочна мережа, коди з максимальною відстанню, блоки підстановки, поле Галуа, довжина слова кода, твірна матриця.

ВСТУП

Проблема підвищення швидкості реалізації методів захисту інформації в комп`ютерних мережах та системах та їхніх криптографічних показників є актуальною проблемою по причині постійного збільшення обсягу передавання інформації каналами зв`язку та спроб несанкціонованого доступу до ресурсів комп`ютерних систем.

Багато сучасних алгоритмів шифрування базуються на архітектурі підстановочно-перестановочних мереж (Substitution-Permutation Network-SPN) та їхніх модифікацій – гніздових SPN мереж (nested SPN) [1, 2]. Одним з критичних компонентів цих мереж є блок підстановки (Substitution Box – S-box). Криптографічна стійкість S-боксу, яка впливає на криптографічну стійкість всього шифру, прямо пропорційна його розміру [3]. Тому застосування SPN-мереж з S-боксами розмір яких більше за розмір S-боксів сучасних алгоритмів шифрування підвищить криптографічну стійкість всього шифру. Широкого розповсюдження, в сучасних алгоритмах шифрування на основі SPN набули S-бокси розміром 4х4 біт та 8х8 біт [1, 2]. Таке обмеження розміру S-боксу в свій час було обумовлене малим обсягом оперативної пам`яті комп`ютерної системи. Тенденції розвитку сучасної комп`ютерної промисловості демонструють збільшення розміру оперативної пам`яті в декілька раз. Тому існує доцільність розглянути реалізацію та обчислювальні показники в комп`ютерній системі SPN-мережі, яка використовує S-бокси більшого розміру (наприклад 16х16 біт).

В наступних роботах [4, 5] отримані окремі результати по використанню S-боксів розміром 16х16 біт в блочних шифрах. В роботі [4] наведені показники протидії до диференційного та лінійного криптаналізу шифру, який створений на основі архітектури мережа Фейстеля та використовує S-бокси розміром 16х16 біт. В роботі [5] визначені окремі показники стійкості блоків підстановки розміром 16х16 біт. Але в цих роботах відсутнє визначення обчислювальних показників як окремих частин шифру так і шифру в цілому.

Дослідження обчислювальних показників шифру, створеного на основі гніздової SPN-мережі яка використовує S-бокси розміром 16х16 біт є відкритим питанням. Тому метою цієї статті є визначення необхідного розміру оперативної пам`яті, швидкості реалізації шифровального перетворення створеного на основі з S-боксами розміром 16х16 біт.

ПОСТАНОВКА ЗАВДАННЯ

Гніздова SPN-мережа має найвищі показники протидії до лінійного та диференційного криптаналізу, якщо на нижньому та верхньому рівні використовує коди з максимальною відстанню

(КМВ-перетворення) [6]. Програмна реалізація КМВ-перетворення виконується як добуток матриць в полі Галуа, що вимагає певну кількість модульних добутків та певну кількість операцій XOR над послідовностями, які мають розмір елемента поля. На різних платформах комп`ютерних систем кількість тактів для виконання таких операцій має різну кількість. Для загального способу реалізації КМВ-перетворення на різних платформах комп`ютерних систем слід використовувати уніфікований та загальний спосіб реалізації – табличні підстановки. Тоді кількість підстановок буде визначати швидкість шифрування, а розмір таблиць - об`єм пам`яті. Розв`язок завдання представимо в чотирьох кроках. На першому кроці розглянемо операції, що відбуваються на двох рівнях гніздової SPN-мережі з застосуванням перетворення КМВ. На другому кроці визначимо операції, які можна виконати табличнимии підстановками. На третьому кроці визначимо чинники, від яких залежить кількість підстановок. На четвертому кроці визначимо кількість табличних підстановок, що мають використовуватися для реалізації гніздових SPN-мереж з S-боксами розміром 16x16 різного типу, відповідний обсяг пам`яті та з`ясуємо найбільш придатний варіант реалізації SPN-мережі в комп`ютерній системі з урахуванням необхідної пам`яті та швидкості роботи.

РОЗВ`ЯЗАННЯ

Згідно першого кроку для визначення кількості операцій підстановки на двох рівнях (нижньому та верхньому) гніздової SPN-мережі необхідно розглянути математичні операції, які в ній відбуваються. На цих рівнях виконуються перетворення реалізовані кодами з максимальною відстанню.

Код КМВ ($2m$, m, m+1) – код з твірною матрицею $G = [I] \cdot [C]$, де C – матриця розміром m x m, а I – одинична матриця. Для формування перетворення в шифрах на основі SPN-мереж застосовується лише матриця – C.

Перетворення, що відбувається на одному рівні гніздової SPN згідно КМВ визначає відображення результатів S-боксів X в вектор Y через добуток матриць над полем Галуа – $GF(2^n)$. Параметр n визначає довжину S-боксу

$$\begin{bmatrix} y_0 \\ \cdot \\ \cdot \\ \cdot \\ y_{m-1} \end{bmatrix} = \begin{bmatrix} c_{0,0} \ldots c_{0,m-1} \\ c_{ij} \\ c_{m-1,0} \ldots c_{m-1,m-1} \end{bmatrix} \times \begin{bmatrix} x_0 \\ \cdot \\ \cdot \\ \cdot \\ x_{m-1} \end{bmatrix}, \quad (1)$$

де x_j - результуюче значення певного S-боксу, $x_i \in GF(2^n)$; y_j -результуюче значення певного рівня гніздової SPN, $y_i \in GF(2^n)$; c_{ij} - коефіцієнти твірної матриці КМВ-перетворення $c_{ij} \in GF(2^n)$; m-довжина слова КМВ.

В відповідності другого кроку визначимо, яким чином можна реалізувати вираз (1) табличними підстановками. Згідно добутку матриць перетворимо вираз (1) до виразу

$$\begin{bmatrix} y_0 \\ \cdot \\ \cdot \\ \cdot \\ y_{m-1} \end{bmatrix} = \begin{bmatrix} c_{0,0} \\ \cdot \\ \cdot \\ \cdot \\ c_{m-1,0} \end{bmatrix} \times x_0 + \ldots \begin{bmatrix} c_{0,m-1} \\ \cdot \\ \cdot \\ \cdot \\ c_{m-1,m-1} \end{bmatrix} \times x_{m-1}. \quad (2)$$

Перетворення (2), що відбувається на одному рівні складається з сукупності m-матриць-стовбців A_j

$$A_j = \begin{bmatrix} c_{0,j} \times x_j \\ \cdot \\ \cdot \\ \cdot \\ c_{m-1,j} \times x_j \end{bmatrix}. \quad (3)$$

А результат одного рівня визначається виразом

$$\begin{bmatrix} y_0 \\ \cdot \\ \cdot \\ \cdot \\ y_{m-1} \end{bmatrix} = A_0 + \ldots A_j + \ldots + A_{m-1}. \quad (4)$$

Обчислення кожного доданку A_j залежить від результату певного S-боксу – x_j, та від коефіцієнтів

c_{ij} матриці КМВ. В свою чергу значення x_j залежить від вхідного вектора v_j певного S-боксу. Так як обчислення S-боксу відбувається незмінними виразами і коефіцієнти c_{ij} – константи, то реалізацію доданку A_j табличною підстановкою буде представляти одномірний масив. Індекс цього масиву – v_j, розмір якого дорівнює розміру S-боксу та порядку поля $GF(2^n)$. Елемент масиву – доданок $A_j[v_j]$, розмір якого – добуток порядка поля – n та довжини слова КМВ – m.

Згідно третього кроку визначимо чинники від яких залежить кількість операцій табличних підстановок. Операції табличних підстановок в комп`ютерних системах – це операції читання даних з пам`яті. Кількість операцій читання даних визначається виразом,

$$k = d/w, \tag{5}$$

де d – довжина даних (біт), w – довжина слова комп`ютерної системи (біт).

Тоді кількість операцій читання для реалізації табличними підстановками виразу (4) буде дорівнювати

$$k = d*m/w = m^2n/w \tag{6}$$

Так як довжина m слова коду з максимальною відстанню та порядок поля – n, залежить від типу гніздової SPN-мережі, то як визначено на четвертому кроці, необхідно розглянути всі можливі типи гніздових SPN-мереж довжиною 128 біт з S-боксами розміром 16 х 16. Можливі 4 типи таких мереж.

В мережі першого типу КМВ перетворення низького рівня формується векторами x y, та c

$$X = x; \quad Y = y; \quad C = c, \tag{7}$$

де $x, y, cGF(2^{16})$.

Для такого коду довжина слова m = 1, порядок поля n = 16. Згідно виразу (6) – кількість підстановок дорівнює 1.

КМВ перетворення високого рівня – матрицями

$$X = \begin{bmatrix} x_0 \\ \vdots \\ x_7 \end{bmatrix}; \qquad Y = \begin{bmatrix} y_0 \\ \vdots \\ y_7 \end{bmatrix}; \qquad C = \begin{bmatrix} c_{0,0} & \dots & c_{0,7} \\ & c_{ij} & \\ c_{7,0} & \dots & c_{7,7} \end{bmatrix}, \tag{8}$$

де x_i, y_i, c_{ij} $GF(2^{16})$.

Для такого коду m_1 = 8, n = 16. Згідно виразу (6) кількість підстановок становить 16. Сукупна кількість підстановок для реалізації двох рівнів – 17.

В мережі другого типу КМВ перетворення низького рівня формується матрицями

$$X = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}; \qquad Y = \begin{bmatrix} y_0 \\ y_1 \end{bmatrix}; \qquad C = \begin{bmatrix} c_{0,0} & c_{0,1} \\ c_{1,0} & c_{1,1} \end{bmatrix}, \tag{9}$$

де x_i, y_i, c_{ij} $GF(2^{16})$.

Для такого коду довжина слова m2 = 2, n = 16. Згідно виразу (6) кількість підстановок становить 1.

КМВ перетворення високого рівня – матрицями

$$X = \begin{bmatrix} x_0 \\ \vdots \\ x_3 \end{bmatrix}; \qquad Y = \begin{bmatrix} y_0 \\ \vdots \\ y_3 \end{bmatrix}; \qquad C = \begin{bmatrix} c_{0,0} & \dots & c_{0,3} \\ & c_{ij} & \\ c_{3,0} & \dots & c_{3,3} \end{bmatrix}, \tag{10}$$

де x_i, y_i, c_{ij} $GF(2^{32})$.

Для такого коду m_1 = 4, n = 32. Кількість підстановок становить 8. Сукупна кількість підстановок

для реалізації двох рівнів – 9.

В мережі третього типу КМВ перетворення низького рівня формується матрицями :

$$X = \begin{bmatrix} x_0 \\ \cdot \\ \cdot \\ \cdot \\ x_3 \end{bmatrix}; \qquad Y = \begin{bmatrix} y_0 \\ \cdot \\ \cdot \\ \cdot \\ y_3 \end{bmatrix}; \qquad C = \begin{bmatrix} & & \\ c_{0,0} & \dots & c_{0,3} \\ & & \\ \cdot & c_{ij} & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ & & \\ c_{3,0} & \dots & c_{3,3} \end{bmatrix}, \tag{11}$$

де x_i, y_i, c_{ij} $GF\left(2^{16}\right)$.

Для такого коду довжина слова $m_2 = 4$, $n = 16$. Кількість підстановок становить 4.

КМВ перетворення високого рівня – матрицями:

$$X = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}; \qquad Y = \begin{bmatrix} y_0 \\ y_1 \end{bmatrix}; \qquad C = \begin{bmatrix} c_{0,0} & c_{0,1} \\ c_{1,0} & c_{1,1} \end{bmatrix}. \tag{12}$$

де x_i, y_i, c_{ij} $GF\left(2^{64}\right)$.

Для такого коду $m_2 = 2$, $n = 64$. Кількість підстановок становить 8. Сукупна кількість підстановок для реалізації двох рівнів – 12.

В мережі четвертого типу КМВ перетворення низького рівня формується матрицями

$$X = \begin{bmatrix} x_0 \\ \cdot \\ \cdot \\ \cdot \\ x_7 \end{bmatrix}; \qquad Y = \begin{bmatrix} y_0 \\ \cdot \\ \cdot \\ \cdot \\ y_7 \end{bmatrix}; \qquad C = \begin{bmatrix} & & \\ c_{0,0} & \dots & c_{0,7} \\ & & \\ \cdot & c_{ij} & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ & & \\ c_{7,0} & \dots & c_{7,7} \end{bmatrix}. \tag{13}$$

де x_i, y_i, c_{ij} $GF\left(2^{16}\right)$.

Для такого коду довжина слова $m_2 = 8$, $n = 16$. Кількість підстановок становить 16.

КМВ перетворення високого рівня – векторами x, y та c

$$X = x; \quad Y = y; \quad C = c, \tag{14}$$

де x, y, c $GF\left(2^{128}\right)$.

Для такого коду $m_1 = 1$, $n = 128$. Кількість підстановок становить 2. Сукупна кількість підстановок для реалізації двох рівнів – 18.

В таблиці 1 наведені варіанти гніздових SPN, тип КМВ-кодів верхнього та нижнього рівнів, та розрахована за виразом (6) відповідна кількість операцій підстановок в 64-ох розрядних системах для реалізації двох послідовних рівнів.

Таблиця 1.

Варіанти гніздових SPN-мереж з S-боксами розміром 16x16 та відповідна кількість операцій підстановки

Номер варіанту	Тип КМВ нижнього рівня	Тип КМВ верхнього рівня	Кількість підстановок
1	(2, 1, 2)	(16, 8, 9)	17
2	(4, 2, 3)	(8, 4, 5)	9
3	(8, 4, 5)	(4, 2, 3)	8
4	(16, 8, 9)	(2, 1, 2)	18

З аналізу таблиці 1 очевидно, що найменшу кількість підстановок та найбільшу швидкість реалізації мають SPN-мережі варіанту 2 та 3. Найменша кількість підстановок для реалізації SPN-мереж такої довжини з S-боксами розміру 8x8 становить 32 [7]. Тоді реалізація SPN-мереж з S-боксами

розміром 16x16 біт збільшує швидкість в 1,7-4 рази по зрівнянню з мережами, що використовують S-бокси розміром 8x8 біт. Але крім швидкості реалізації іншим критичним обчислювальним критерієм є необхідний обсяг пам`яті. Визначимо необхідний обсяг пам`яті для реалізації визначених вище типів SPN-мереж табличними підстановками.

Розмір необхідної пам`яті дорівнює розміру таблиці підстановки. Ця таблиця реалізується в вигляді масиву. Індекс масиву та елемент масиву це відповідно значення $v_i$ та $A_j[v_j]$. Тоді для реалізації одного матриці стовпця $A_j[v_j]$ необхідно мати пам`ять

$$V=2^n nm/8 \text{ [байт]}. \quad (15)$$

де n – порядок поля; m – довжина слова.

Реалізації одного рівня SPN – мережі вимагає використати m різних матриць стовпців. Тоді весь необхідний обсяг пам`яті для реалізації одного рівня табличними підстановками визначається виразом:

$$V=2^n nm^2/8 \text{ [байт]}. \quad (16)$$

Загальний обсяг пам`яті для реалізації двох рівнів гніздової SPN – мережі буде визначатися виразом

$$V=2^n n_н m_н{}^2/8 + 2^n n_в m_в{}^2/8 \text{ [байт]}, \quad (17)$$

де $n_н$ – порядок поля нижнього рівня; $m_н$ – довжина слова КМВ нижнього рівня; $n_в$ – порядок поля верхнього рівня; $m_в$ – довжина слова КМВ верхнього рівня.

В таблиці 2 наведені варіанти гніздових SPN-мереж з S-боксами розміром 16x16 біт, відповідні типи КМВ-кодів верхнього та нижнього рівнів, та розрахований за виразом (17) необхідний обсяг пам`яті для реалізації двох послідовних рівнів цих мереж табличними підстановками.

Таблиця 2.

Варіанти гніздових SPN-мереж з S-боксами розміром 16x16 та необхідний обсяг пам`яті для їх реалізації табличними підстановками

Номер варіанту	Тип КМВ нижнього рівня	Тип КМВ верхнього рівня	Необхідний обсяг пам`яті (байт)
1	(2, 1, 2)	(16, 8, 9)	8519680
2	(4, 2, 3)	(8, 4, 5)	274878431232
3	(8, 4, 5)	(4, 2, 3)	2^{69}
4	(16, 8, 9)	(2, 1, 2)	2^{132}

З аналізу значень обсягу пам`яті необхідного для реалізації SPN-мережі табличними підстановками, отриманих в таблиці 2, зрозуміло, що при сучасному розвитку комп`ютерних систем та мереж найбільш придатною для реалізації є SPN-мережа варіанту 1 реалізаця інших типів мереж вимагає обсяг пам`яті несумірний з обсягом пам`яті сучасної комп`ютерної системи. SPN-мережа варіанту 1 вимагає приблизно об`єм 8 Мбайт, що становить лише дві сторінки пам`яті великого розміру, або приблизно 0,2% від пам`яті ОЗП, яка потрібна для роботи ОС Windows 7. Для реалізації двох рівнів такої SPN-мережі в комп`ютерній системі табличними підстановками необхідно виконати 17 операцій читання з пам`яті. Тобто застосування мережі такого типу збільшує швидкість роботи приблизно в 1,8 рази по зрівнянню з SPN-мережами, що містять S-бокси розміром 8x8 біт.

ВИСНОВКИ

В ході проведенного дослідження визначено обчислювальні характеристики гніздових SPN-мереж довжиною 128 біт та розміром S-боксів 16x16 біт. Отримані значення обсягу необхідної пам`яті та кількість операцій табличних підстановок для реалізації двох рівнів гніздових SPN-мереж з S-боксами розміром 16x16 біт різного типу. Аналіз отриманих показників демонструє, що найбільш придатною (з урахуванням пам`яті та швидкості) для реалізації в комп`ютерних системах та мережах є гніздова SPN-мережа 1 варіанту. При застосуванні такої архітектурі в блочному шифрі швидкість його реалізації в комп`ютерній системі збільшується приблизно в 1,8 рази або на 80%. В якості подальших досліджень необхідно визначити показники ефективності застосування такого перетворення в комп`ютерній системі з урахуванням криптографічних показників та визначити перетворення, що мають виконуватися в S-боксах такого розміру.

СПИСОК ЛІТЕРАТУРИ

1. Daemen J. The Design of Rijndael. AES: The Advanced Encryption Standard / Joahn Daemen, Vincent Rijmen // Springer – Berlin.- 2002. – V.234. – P. 24 – 28.
2. The block cipher Hierocrypt /[Ohkuma K., Muratani H., Sano F., Kawamura S]. // Proceedings of Selected Areas in Cryptography - SAC 2000, Lecture Notes in Computer Science. - Springer-Verlag.- 2001. - Vol. 2012. - P. 72–88.
3. O'Connor L. On the distribution of characteristics in bijective mappings / O'Connor L. // Advances in Cryptology – EUROCRYPT '93. – Springer- Verlag. – 1994. – Vol.678. – P. 360–370.
4. The new variable-length key symmetric cryptosystem [Rezaei P., Rushdan S., Mohd A., Mohamed O.]. – www .scipub.org/fulltext/jms2/jms25124-31.pdf
5. Ростовцев А. Большие подстановки для программных шифров / А. Ростовцев // Проблемы информационной безопасности. Компьютерные системы . - 2000. - № 3. – С. 31–35
6. Kanda M. Practical security evaluation against differential and linear cryptanalysis for Feistel ciphers with SPN round function. / Kanda M. // Seventh Annual International Workshop on Selected Areas in Cryptography-SAC`00, Lecture Notes in Computer Science – Springer-Verlag. – 2001. -Vol. 2012. – P.324-338
7. Бевз О.М. Методи шифрування на основі високонелінійних бульових функцій та кодів з максимальною відстанню: дис. ... канд. техн. наук: 05.13.05 / Бевз Олександр Миколайович – Вінниця: 2008. -181 с.

Надійшла до редакції 11.03.2011р.

Бевз О.М. – к.т.н., старший викладач, кафедри АІВТ, Вінницький національний технічний університет, Україна