УДК 681.3.06

Бевз О.М., Папінов В.М.

КРИПТОГРАФІЧНІ ПОКАЗНИКИ ГНІЗДОВИХ SPN-МЕРЕЖ З S-БОКСАМИ РОЗМІРОМ 16×16 БІТ

В статті визначено криптографічну стійкість гніздових підстановочно-перестановочних мереж довжиною 128 біт та розміром S-боксів 16×16 біт по відношенню до лінійного та диференційного криптаналізу. Визначення показників стійкості проводилося по кількості активних S-боксів одного раунду SPN-мережі та нижній межі диференційної та лінійної характеристики S-боксу.

Ключові слова: криптографічна стійкість, гніздова підстановочно-перестановочна мережа, блоки підстановки, код з максимальною відстанню, активний S-бокс.

Вступ. Проблема підвищення криптографічних показників методів захисту інформації є актуальною проблемою. Кожну годину в мережі INTERNET та локальних мережах виникає велика кількість випадків проникнення сторонніх осіб до носіїв даних. Причина цього недосконаліть алгоритмів шифрування, що застосовуються в протоколах мереж TCP-IP. Недосконаліть алгоритмів є наслідком низької стійкості криптографічних перетворень, з яких складається алгоритми шифрування. Тому формування перетворень, в яких відсутні дані недоліки є актуальною задачею.

Багато сучасних алгоритмів блочного шифрування базуються на архітектурі підстановочно-перестановочних мереж (Substitution-Permutation Network – SPN) та їхніх модифікацій гніздових підстановочно-перестановочних мереж (nested SPN) [1-3]. В своїй структурі ці мережи в якості частин розсіювання використовують блоки підстановки (Substitution Box – S-box). Критичним чинником S-боксу, від якого залежить стійкість всієї системи є його розмір [4]. Широкого розповсюдження, в сучасних алгоритмах шифрування на основі SPN набули S-бокси розміром 4×4 біт та 8×8 біт [1-3]. Дослідження впливу властивостей S-боксів більшого розміру на властивості шифру, що базується на архітектурі гніздових підстановочно-перестановочних мереж, є актуальним питанням.

В наступних роботах отримані окремі результати по визначенню властивостей S-боксів розміром 16×16 біт та їхній вплив на стійкість всього шифру. В роботі [5] наведені властивості шифру, який створений на основі архітектури мережа Фейстеля та використовує S-бокси розміром 16×16 біт. В роботі [6] визначені окремі показники стійкості блоків підстановки розміром 16×16 біт, але не визначена стійкість шифру, який має їх використовувати.

Дослідження показників стійкості шифру, створеного на основі гніздових SPN-мереж, та які використовують S-бокси розміром 16×16, є відкритим питанням. Тому метою цієї статті є визначення криптографічних характеристик шифровального перетворення створеного на основі гніздової SPN мережі з S-боксами розміром 16×16 біт.

Постановка завдання. Криптографічна стійкість шифру, що створений на основі підстановочно-перестановочних мереж є результатом стійкості його окремих частин – раундів. Стійкість одного раунду до диференційного та лінійного криптаналізу головним чином залежить від двох чинників – кількості активних S-боксів та ймовірності диференційної або лінійної характеристики (лінійної оболонки) [7]. В свою чергу ці чинники залежать від типу мережі [8]. Реалізацію завдання по визначенню впливу S-боксів розміром 16×16 на стійкість окремих раундів шифру реалізуємо трьома кроками. На першому кроці визначимо типи можливих гніздових SPN-мереж довжиною 128 біт та розмірорм S-боксу 16 біт. На другому кроці визначимо кількість активних S-боксів гніздової SPN-мережі певного типу. На третьому кроці визначимо кількісні показники стійкості одного раунду гніздової SPN-мережі, що складається з нижнього та верхнього рівнів.

Розв`язання. Гніздова SPN-мережа представляє собою перетворення, що складається з двох рівнів – верхнього та нижнього (рисунок 1).

На нижньому рівні виконується перетворення S-боксом одного розміру, на верхньому рівні застосовується перетворення S-боксом іншого розміру. Кожний S-бокс верхнього рівня – це SPN-мережа малого розміру на верхньому рівні.

Для реалізації максимальної кількості активних S-боксів в якості лінійного перетворення на верхньому та нижньому рівнях застосовуються перетворення сформовані кодами з максимальною відстанню, $КМВ_н$ та $КМВ_в$ відповідно [9]. Для SPN-мережі такого типу кількість активних S-боксів дорівнює

$$N = (m_2 + 1)(m_1 + 1), \tag{1}$$

де m_2 – довжина слова $КМВ_н$,
m_1 – довжина слова $КМВ_в$.

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

Код КМВ визначає відображення входу X в вихід Y через добуток матриць над полем Галуа – $GF(2^n)$:

$$X = C \cdot A \tag{2}$$

де

$$X = \begin{bmatrix} x_0 \\ . \\ . \\ . \\ x_{m-1} \end{bmatrix}, \qquad Y = \begin{bmatrix} y_0 \\ . \\ . \\ . \\ y_{m-1} \end{bmatrix}, \qquad C = \begin{bmatrix} & & \\ c_{n-1,n-1} & \cdots & c_{n-1,0} \\ . & c_{ij} & . \\ . & & . \\ . & & . \\ c_{0,n-1} & \cdots & c_{0,0} \end{bmatrix} \tag{3}$$

Елементи матриць $x_0, y_0, c_{ij} \in GF(2^n)$.

Кожна колонка матриці C визначається виразом:

$$c_{n\text{-}1,j} \cdot x^{n-1} + \ldots + c_{0j} = x^j (f_{n-1} \cdot x^{n-1} + \ldots f_0) \bmod P(x) \tag{4}$$

де $f_{n-1} \cdot x^{n-1} + \ldots f_0$ – константа добутку.

Так як довжина слова коду з максимальною відстанню, що застосовується в гніздовій SPN-мережі залежить від типу мережі, то в відповідності кроку 1 необхідно розглянути всі можливі типи гніздових SPN-мереж довжиною 128 біт з S-боксами розміром 16×16. Можливі 4 типи таких мереж.

В мережі першого типу КМВ перетворення низького рівня формується матрицями-стовпцями x та y, та матрицею C :

$$X = x_0, \quad Y = y_0, \quad \tilde{N} = c_0 \tag{5}$$

де $x_0, y_0, c_0 \in GF\left(2^{16}\right)$.

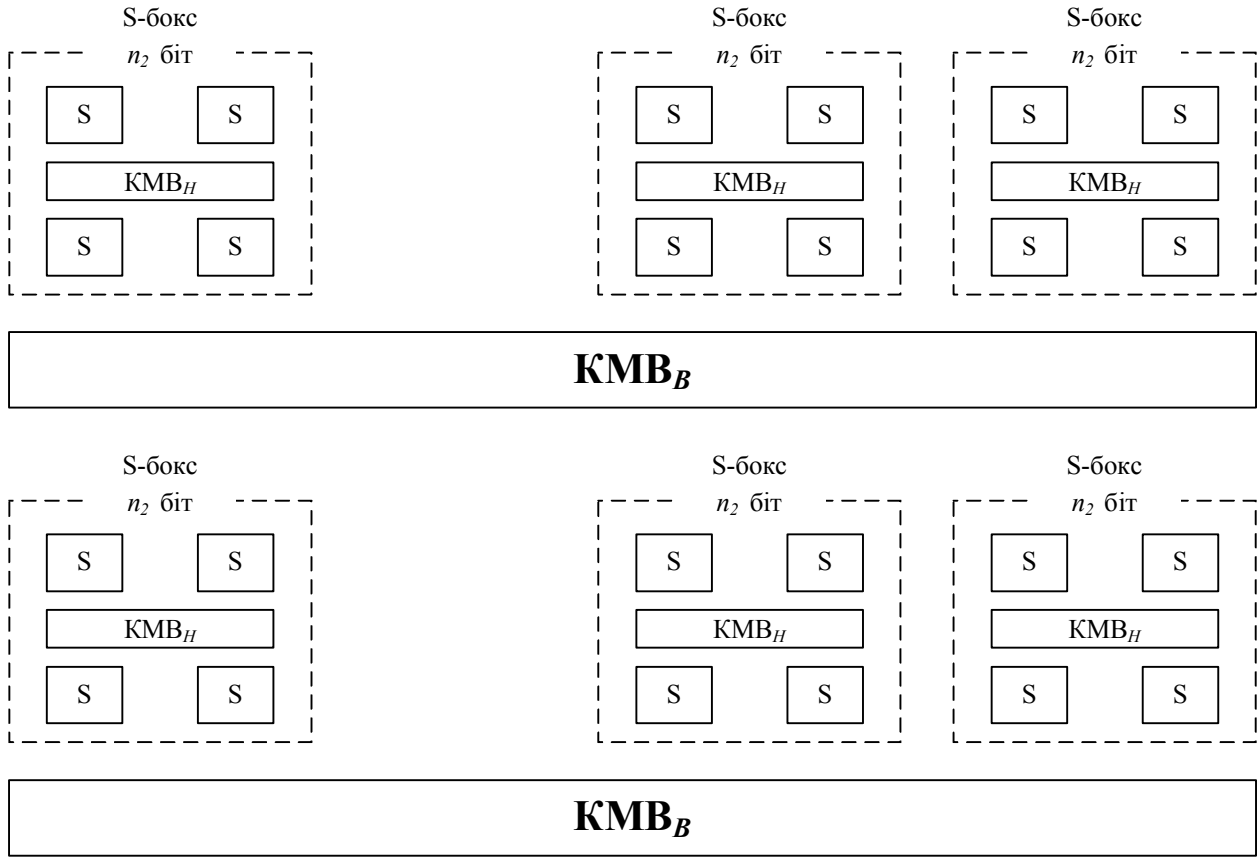

Рис. 1 Гніздова SPN-мережа

Для такого коду довжина слова $m_2 = 1$.

КМВ перетворення високого рівня – матрицями:

$$X = \begin{bmatrix} x_0 \\ . \\ . \\ . \\ x_7 \end{bmatrix}, \qquad Y = \begin{bmatrix} y_0 \\ . \\ . \\ . \\ y_7 \end{bmatrix}, \qquad C = \begin{bmatrix} & & \\ & & \\ c_{0,0} & \cdots & c_{0,7} \\ . & c_{ij} & . \\ . & & . \\ . & & . \\ c_{7,0} & \cdots & c_{7,7} \end{bmatrix} \tag{6}$$

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

Для такого коду $m_1 = 8$.

В мережі другого типу КМВ перетворення низького рівня формується матрицями :

$$X = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}, \qquad Y = \begin{bmatrix} y_0 \\ y_1 \end{bmatrix}, \qquad C = \begin{bmatrix} c_{0,0} & c_{0,1} \\ c_{1,0} & c_{1,1} \end{bmatrix} \tag{7}$$

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

Для такого коду довжина слова $m_2 = 2$.

КМВ перетворення високого рівня – матрицями :

$$X = \begin{bmatrix} x_0 \\ . \\ . \\ . \\ x_3 \end{bmatrix}, \qquad Y = \begin{bmatrix} y_0 \\ . \\ . \\ . \\ y_3 \end{bmatrix}, \qquad C = \begin{bmatrix} & & \\ & & \\ c_{0,0} & \cdots & c_{0,3} \\ . & c_{ij} & . \\ . & & . \\ . & & . \\ c_{3,0} & \cdots & c_{3,3} \end{bmatrix} \tag{8}$$

де $x_i, y_i, c_{ij} \in GF\left(2^{32}\right)$

Для такого коду $m_1 = 4$.

В мережі третього типу КМВ перетворення низького рівня формується матрицями :

$$X = \begin{bmatrix} x_0 \\ . \\ . \\ . \\ x_3 \end{bmatrix}, \qquad Y = \begin{bmatrix} y_0 \\ . \\ . \\ . \\ y_3 \end{bmatrix}, \qquad C = \begin{bmatrix} & & \\ & & \\ c_{0,0} & \cdots & c_{0,3} \\ . & c_{ij} & . \\ . & & . \\ . & & . \\ c_{3,0} & \cdots & c_{3,3} \end{bmatrix} \tag{9}$$

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

Для такого коду довжина слова $m_2 = 4$.

КМВ перетворення високого рівня – матрицями:

$$X = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}, \qquad Y = \begin{bmatrix} y_0 \\ y_1 \end{bmatrix}, \qquad C = \begin{bmatrix} c_{0,0} & c_{0,1} \\ c_{1,0} & c_{1,1} \end{bmatrix} \tag{10}$$

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

Для такого коду $m_2 = 2$.

В мережі четвертого типу КМВ перетворення низького рівня формується матрицями:

$$X = \begin{bmatrix} x_0 \\ . \\ . \\ . \\ x_7 \end{bmatrix}, \qquad Y = \begin{bmatrix} y_0 \\ . \\ . \\ . \\ y_7 \end{bmatrix}, \qquad C = \begin{bmatrix} & & \\ c_{0,0} & \cdots & c_{0,7} \\ . & c_{ij} & . \\ . & & . \\ . & & . \\ c_{7,0} & \cdots & c_{7,7} \end{bmatrix} \tag{11}$$

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

Для такого коду довжина слова $m_2 = 8$.

КМВ перетворення високого рівня – матрицями-стовпцями *x* та *y*, та матрицею *C*

$$X = x_0, \quad Y = y_0, \quad \tilde{N} = c_0 \tag{12}$$

де $x_i, y_i, c_{ij} \in GF\left(2^{128}\right)$.

Для такого коду $m_1 = 1$.

В таблиці 1 наведені варіанти гніздових SPN, тип КМВ-кодів верхнього та нижнього рівнів, та розрахована за виразом (1) відповідна кількість активних S-боксів, що створюються мережею певного типу для S-боксів розміром 16×16 для довжини SPN-мережі 128 біт.

Таблиця 1

Варіанти гніздових SPN-мереж з S-боксами розміром 16×16 та відповідна кількість активних S-боксів

Номер варіанту	Тип КМВ нижнього рівня	Тип КМВ верхнього рівня	Кількість активних S-боксів
1	(2, 1, 2)	(16, 8, 9)	18
2	(4, 2, 3)	(8, 4, 5)	15
3	(8, 4, 5)	(4, 2, 3)	15
4	(16, 8, 9)	(2, 1, 2)	18

З аналізу табл. 1 очевидно, що найбільшу кількість активних S-боксів мають варіанти 1 та 4 SPN-мереж. Але крім кількості активних S-боксів раунду, стійкість раундового перетворення залежить від значення ймовірності лінійної *Q* та диференційних *q* характеристик S-боксів, що застосовуються в раунді [7].

Ймовірність диференційної характеристики раунду визначається виразом:

$$P = p_s^n \tag{13}$$

де p_s – ймовірності диференційної характеристики S-боксу, що застосований в раунді;

n – кількість активних S-боксів в раунді.

Ймовірності лінійної характеристики раунду визначається виразом (14)

$$Q = p_s^n \tag{14}$$

де q_s – ймовірності лінійної характеристики S-боксу, що застосований в раунді; *n* – кількість активних S-боксів в раунді.

Визначимо значення виразів (13)-(14) по нижній межі ймовірності лінійної та диференційної характеристик. Як визначено в роботі [4] нижня межа диференційної та лінійної характеристики S-боксу розміром $n \times n$ визначається виразом:

$$q_S = p_S = \frac{n}{2^{n-1}} \tag{15}$$

де n – розмір S-боксу.

З виразу (15) випливає, що для S-боксів розміром 16×16 біт, ймовірність лінійної оболонки q_S та ймовірність диференційної характеристики p_S дорівнює 2^{-11}.

Визначимо значення ймовірностей диференційної та лінійної характеристик для гніздових SPN-мереж згідно виразів (13)-(14) та представимо їх в таблиці 2.

Таблиця 2

Варіанти гніздових SPN-мереж з S-боксами розміром 16×16 та відповідне значення ймовірностей лінійної та диференційної характеристики для одного раунду

Номер варіанту	Тип КМВ нижнього рівня	Тип КМВ верхнього рівня	Значення ймовірності	Стійкість
1	(2, 1, 2)	(16, 8, 9)	2^{-198}	198
2	(4, 2, 3)	(8, 4, 5)	2^{-165}	165
3	(8, 4, 5)	(4, 2, 3)	2^{-165}	165
4	(16, 8, 9)	(2, 1, 2)	2^{-198}	198

Для прикладу порівняємо отримані значення стійкості зі стійкістю одного раунду гніздових SPN-мереж з S-боксами розміром 8×8. З виразу (15) випливає, що нижня межа стійкості дорівнює 2^{-4}. Для гніздових SPN-мереж з S-боксами розміром 8x8 максимально можлива кількість активних S-боксів дорівнює 34. З виразів (13)-(14) отримаємо, що стійкість одного раунду такої мережі становить 136. Що приблизно в 1,5 рази менше за стійкість гніздової SPN-мережі з S-боксами розміром 16 біт.

Висновки. В ході проведенного дослідження визначено диференційні та лінійні характеристики гніздових SPN-мереж довжиною 128 біт та розміром S-боксів 16×16 біт. Отримані показники стійкості відносно диференційного та лінійного криптаналізу демонструють, що застосування в гніздовій SPN-мережі S-боксів розміром 16×16 біт підвищує стійкість перетворення по відношенню до SPN-мережі з S-боксами розміром 8×8 біт приблизно в 1,5 рази. В якості подальших досліджень необхідно визначити обчислювальні показники реалізації гніздової SPN-мережі такого типу в комп`ютерній системі та показники ефективності застосування такого перетворення в комп`ютерній системі.

ЛІТЕРАТУРА

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. The cipher SHARK [Rijmen V., Daemen J., Preneel B., Bosselaers A., Win E] // Proceedings of Fast Software Encryption - FSE'96, Lecture Notes in Computer Science. - Springer-Verlag. – 1997. - Vol. 1039. - P. 99–112

4. 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.

5. The new variable-length key symmetric cryptosystem [Rezaei P., Rushdan S., Mohd A., Mohamed O.]. – www .scipub.org/fulltext/jms2/jms25124-31.pdf

6. Ростовцев А. Большие подстановки для программных шифров / Ростовцев А. // Проблемы информационной безопасности. Компьютерные системы . - 2000. - № 3. – С. 31–35

7. Biham E. On Matsui`s linear cryptanalysis / Biham E. // Advances in Cryptology – EUROCRYPT `94. – Lecture Notes in Computer Science – Springer-Verlag. – 1995. – Vol. 950. – P.341-355.

8. 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.

9. 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

Надійшла: 27.09.2011

Рецензент: д.т.н., проф. Корченко О.Г.