

Захист інформації в інформаційно-телекомунікаційних системах

УДК 681.3.06

О.М. Бевз, В.М. Папінов

Вінницький національний технічний університет, Вінниця

ВИЗНАЧЕННЯ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ШИФРУВАННЯ ПІДСТАНОВОЧНО-ПЕРЕСТАНОВОЧНИХ МЕРЕЖ З БЛОКАМИ ПІДСТАНОВКИ РОЗМІРОМ 16x16 БІТ В КОМП'ЮТЕРНИХ СИСТЕМАХ

В статті визначено показники ефективності шифрування в 64-ох розрядних комп'ютерних системах криптографічного перетворення довжиною 128 біт, оснований на архітектурі гніздових підстановочно-перестановочних мереж (nested SPN), з блоками підстановки (S-боксами) розміром 16x16 біт. Коефіцієнт ефективності шифрування визначено як результат відношення криптографічної стійкості відносно лінійного та диференційного криптоаналізу до кількості операцій, що необхідно застосувати для реалізації даного перетворення в комп'ютерних системах.

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

Вступ

Проблема підвищення ефективності шифрування в комп'ютерних системах 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 їх криптографічну стійкість. Широкого розповсюдження, в сучасних алгоритмах шифрування на основі SPN набули S-бокси розміром 4x4 біт та 8x8 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 визначити ефективність шифрування в комп'ютерних системах перетворень, які базуються на SPN-мережах з S-боксами більшого розміру (наприклад 16x16 біт).

В наступних роботах [4, 5] отримані окремі результати по використанню S-боквів розміром 16x16

біт в блочних шифрах. В роботі [4] наведені показники протидії до диференційного та лінійного криптоаналізу шифру, який створений на основі архітектури мережа Фейстеля та використовує S-бокси розміром 16x16 біт. В роботі [5] визначені окремі показники стійкості блоків підстановки розміром 16x16 біт. Але в цих роботах відсутнє визначення показників ефективності шифрування в комп'ютерних системах.

Визначення показників ефективності шифрування в комп'ютерних системах криптографічного перетворення, створеного на основі гніздової SPN-мережі з S-боксами розміром 16x16 біт є відкритим питанням. Метою цієї статті є визначення кількісного значення показника ефективності шифрування перетворення в 64-ох бітних комп'ютерних системах криптографічного перетворення, що виконується гніздовою SPN-мережею довжиною 128 біт з S-боксами розміром 16x16 біт.

Постановка завдання

Для визначення ефективності шифрування в комп'ютерних системах підстановочно-перестановочних мереж слід визначити коефіцієнт, який буде пов'язувати криптографічні показники з часом, який необхідно витратити, на виконання в комп'ютерних системах цього перетворення. Найважливішим криптографічним показником є стійкість до певного типу криптоаналізу. Найпотужнішими типами криптоаналізу є лінійний та диференційний. Тому доцільно визначити саме стійкість гніздової SPN-мережі з S-боксами

розміром 16x16 до цих типів криптоаналізу. Час, який слід витратити, на обчислювальне перетворення залежить від швидкості реалізації цього перетворення в комп'ютерній системі. Перетворення, що відбувається на верхньому та нижньому рівнях, гніздової SPN-мережі містять операції, що вимагають різну кількість тактів процесора на різних платформах комп'ютерних систем. Ефективність шифрування гніздових SPN в комп'ютерних системах має бути компромісним варіантом від стійкості гніздової SPN-мережі та швидкості її реалізації в комп'ютерній системі. Для загального способу реалізації SPN-мережі на різних платформах комп'ютерних систем слід використовувати уніфікований та загальний спосіб реалізації – табличні підстановки. Тоді кількість підстановок буде визначати швидкість шифрування [6]. З урахуванням вищенаведеного коефіцієнт ефективності реалізації α визначається виразом.

$$\alpha = \varepsilon / N, \tag{1}$$

де ε – криптографічна стійкість; N – кількість табличних підстановок.

Розв'язок завдання представимо в двох кроках. На першому кроці визначимо стійкість двох рівнів гніздових SPN-мереж з S-боксами розміром 16x16 біт до лінійного та диференційного криптоаналізу. На другому кроці визначимо кількість табличних підстановок та коефіцієнти ефективності шифрування двох рівнів SPN-мереж з S-боксами розміром 16x16 біт в комп'ютерних системах

Розв'язання

Криптографічна стійкість перетворення до лінійного та диференційного криптоаналізу є функцією від кількості активних S-боксів [7]. Для формування максимальної кількості активних S-боксів на двох рівнях SPN-мережі (верхньому та нижньому) необхідно застосовувати коди з максимальною відстанню - KMB_n та KMB_v . Для SPN-мережі такого типу кількість активних S – боксів дорівнює

$$N = (m_2 + 1)(m_1 + 1), \tag{2}$$

де m_2 – довжина слова KMB_n ; m_1 – довжина слова KMB_v .

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

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

$$\begin{bmatrix} y_0 \\ \vdots \\ y_{m-1} \end{bmatrix} = \begin{bmatrix} c_{0,0} \dots c_{0,m-1} \\ \vdots \\ c_{m-1,0} \dots c_{m-1,m-1} \end{bmatrix} \times \begin{bmatrix} x_0 \\ \vdots \\ x_{m-1} \end{bmatrix}, \tag{3}$$

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 KMB -перетворення $c_{ij} \in GF(2^n)$; m – довжина слова KMB .

Довжина слова коду з максимальною відстанню, що застосовується в гніздовій SPN-мережі залежить від типу мережі, тому слід визначити кількість активних S-боксів для всіх можливих гніздових SPN-мереж довжиною 128 біт з S-боксами розміром 16 x 16. В табл. 1 наведені можливі типи гніздових SPN-мереж довжиною 128 біт з S-боксами розміром 16 x 16 та відповідна кількість активних S-боксів

Таблиця 1

Варіанти гніздових SPN-мереж з S-боксами розміром 16x16 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 гніздових SPN-мереж.

Але крім кількості активних S-боксів раунду, стійкість раундового перетворення залежить від значення ймовірності лінійної p та диференційних q характеристик S-боксів, що застосовуються в раунді [7].

Ймовірність диференційної характеристики раунду визначається виразом:

$$P = p_s^n, \tag{4}$$

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:

$$Q = q_s^n, \tag{5}$$

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

Визначимо значення виразів (4), (5) по нижній межі ймовірності лінійної та диференційної характеристик. Як визначено в роботі [3] нижня межа диференційної та лінійної характеристики S-боксу

розміром $n \times n$ визначається виразом:

$$q_s = p_s = \frac{n}{2^{n-1}}, \quad (6)$$

де n – розмір S-боксу.

З виразу (6) 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 (4), (5) та представимо їх в табл. 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

В відповідності другого кроку визначимо, яким чином можна реалізувати вираз (3) табличними підстановками. Згідно добутку матриць перетворимо вираз (3) до виразу:

$$\begin{bmatrix} y_0 \\ \vdots \\ y_{m-1} \end{bmatrix} = \begin{bmatrix} c_{0,0} \\ \vdots \\ c_{m-1,0} \end{bmatrix} \times x_0 + \dots + \begin{bmatrix} c_{0,m-1} \\ \vdots \\ c_{m-1,m-1} \end{bmatrix} \times x_{m-1} \quad (7)$$

Перетворення (7), що відбувається на одному рівні складається з сукупності m -матриць-стовбців A_j :

$$A_j = \begin{bmatrix} c_{0,j} \times x_j \\ \vdots \\ c_{m-1,j} \times x_j \end{bmatrix} \quad (8)$$

А результат одного рівня визначається виразом:

$$\begin{bmatrix} y_0 \\ \vdots \\ y_{m-1} \end{bmatrix} = A_0 + \dots + A_j + \dots + A_{m-1} \quad (9)$$

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 порядку поля – n та довжини слова КМВ – m .

Операції табличних підстановок в комп'ютерних системах – це операції читання даних з пам'яті.

Кількість операцій читання даних визначається виразом:

$$k = d/w, \quad (10)$$

де d – довжина даних (біт); w – довжина слова комп'ютерної системи (біт).

Тоді кількість операцій читання для реалізації табличними підстановками виразу (9) буде дорівнювати:

$$k = d*m/w = m^2n/w. \quad (11)$$

Для реалізації двох рівнів гніздової SPN-мережі кількість табличних підстановок дорівнює:

$$k = d*m/w = m_n^2n/w + m_b^2n/w, \quad (12)$$

де m_n – довжина слова коду з максимальною відстанню на нижньому рівні гніздової SPN мережі; m_b – довжина слова коду з максимальною відстанню на верхньому рівні гніздової SPN мережі.

В табл. 3 наведені варіанти гніздових SPN, тип КМВ-кодів верхнього та нижнього рівнів, та розрахована за виразом (12) відповідна кількість операцій підстановок в 64-ох розрядних системах для реалізації двох послідовних рівнів.

Таблиця 3

Варіанти гніздових SPN-мереж з S-боксами розміром 16×16 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 табл. 2 очевидно, що найменшу кількість підстановок та найбільшу швидкість реалізації мають SPN-мережі варіанту 2 та 3.

Згідно виразу (1) визначимо показники ефективності реалізації двох рівнів SPN-мереж з S-боксами

розміром 16x16 біт в комп'ютерних системах з довжиною слова 64 біт.

В таблиці 4 наведені варіанти гніздових SPN, тип КМВ-кодів верхнього та нижнього рівнів, та розрахований за виразом (1) показник ефективності реалізації для виконання двох послідовних рівнів.

Таблиця 4

Варіанти гніздових SPN-мереж з S-боксами розміром 16x16 та відповідні показники ефективності реалізації

Номер варіанту	Тип КМВ нижнього рівня	Тип КМВ верхнього рівня	Коефіцієнт ефективності
1	(2, 1, 2)	(16, 8, 9)	11,7
2	(4, 2, 3)	(8, 4, 5)	18,3
3	(8, 4, 5)	(4, 2, 3)	20,6
4	(16, 8, 9)	(2, 1, 2)	11

Чисельні значення показників ефективності реалізації гніздових SPN-мереж з S-боксами розміром 8x8 в 64-ох бітних системах становлять 4,68 – 6,4 [6]. Тоді реалізація SPN-мереж з S-боксами розміром 16x16 біт збільшує показники ефективності в 2,4 – 3,2 рази по зрівнянню з гніздовими SPN мережами, що використовують S-боксы розміром 8x8 біт.

ВИСНОВКИ

В ході проведеного дослідження визначено показники ефективності реалізації двох рівнів гніздових SPN-мереж довжиною 128 біт та розміром S-боксів 16x16 біт в 64-ох розрядних комп'ютерних системах. Отримані чисельні значення коефіцієнтів ефективності демонструють, що застосування в гніздовій SPN-мережі S-боксів розміром 16x16 біт підвищить ефективність реалізації в 64-ох розрядній комп'ютерній системі по відношенню до SPN-мережі з S-боксами розміром 8x8 біт приблизно в

2,4 – 3,2 рази. В якості подальших досліджень необхідно визначити математичні перетворення, що мають відбуватися S-боксами та показники ефективності реалізації шифровального перетворення з певною кількістю раундів в 64-ох розрядній комп'ютерних системі.

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* / K. Ohkuma, H. Muratani, F. Sano, S. Kawamura // *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 [Електронний ресурс]* / P. Rezaei, S. Rushdan, A. Mohd, O. Mohamed. – Режим доступу до ресурсу: 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. Бевз О.М. *Методи шифрування на основі високонелінійних булевих функцій та кодів з максимальною відстанню: дис. ... канд. техн. наук: 05.13.05 / Бевз Олександр Миколайович*. – Вінниця, 2008. – 181 с.
7. Kanda M. *Practical security evaluation against differential and linear cryptanalysis for Feistel ciphers with SPN round function*. / M. Kanda // *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 до редколегії 8.04.2011

Рецензент: д-р техн. наук, проф. В.А. Лужецький, Вінницький національний технічний університет, Вінниця.

ОПРЕДЕЛЕНИЕ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ ШИФРОВАНИЯ ПОДСТАНОВОЧНО-ПЕРЕСТАНОВОЧНЫХ СЕТЕЙ С БЛОКАМИ ПОДСТАНОВКИ РАЗМЕРОМ 16X16 БИТ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

О.М. Бевз, В.М. Папинов

В статье определены показатели эффективности шифрования в 64-ох разрядных компьютерных системах криптографического преобразования длиной 128 бит, использующего архитектуру гnezдовыx подстановочно-перестановочных сетей (nested SPN), с блоками подстановки (S-боксами) размером 16x16 бит. Коэффициент эффективности шифрования определен как результат отношения криптографической стойкости относительно линейного и дифференциального криптоанализа к количеству операций, необходимых для реализации данного преобразования в компьютерных системах.

Ключевые слова: криптографическая стойкость, гnezдовая подстановочно-перестановочная сеть, блоки подстановки, код с максимальным расстоянием

FINDING CHARACTERISTICS OF A EFFECTIVENESS ENCRYPTION SUBSTITUTION-PERMUTATION NETWORKS WITH A 16X16 BITES SUBSTITUTION BOX IN COMPUTER SYSTEMS

O.M. Bevz, B.M. Papinov

There are finding characteristics of a effectiveness encryption in 64-bites computer systems in this note. This encryption based on nested substitution-permutation networks and use 16-bites substitution boxes. The length of this network is 128 bites. The characteristics of the effectiveness encryption finding as a function of a cryptographic security and a number of operations for implementation this transformation in computer systems.

Keywords: cryptographic security, nested substitution-permutation network, substitution box, maximal distance code.