ВОЛОКОННО-ОПТИЧНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНИХ (INTERNET, INTRANET ТОЩО) ТА ЕНЕРГЕТИЧНИХ МЕРЕЖАХ

УДК 681.3.06

О.М. БЕВЗ, В.М. ПАПІНОВ

ВИЗНАЧЕННЯ ПОКАЗНИКІВ ЕФЕКТИВНОСТІ ШИФРУВАННЯ ПІДСТАНОВОЧНО-ПЕРЕСТАНОВОЧНИХ МЕРЕЖ З БЛОКАМИ ПІДСТАНОВКИ ВЕЛИКОГО РОЗМІРУ В ОПТИКО-ЕЛЕКТРОННИХ СИСТЕМАХ

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

Анотація. В данній статті визначені показники ефективності реалізації блочного шифру, який оснований на архітектурі гніздової постановочно-перестановочної мережі (nested SPN) з блоками підстановки (S-боксами) розміром 16x16 біт в оптико-електронних системах. В якості факторів, які визначають ефективність, вибрані швидкість перетворення в оптико-електронній системі і криптографічна стійкість двох послідовних шарів гніздових підстановочно-перестановочних мереж різного типу.

Аннотация. В данной статье определены показатели эффективности реализации блочного шифра, основаного на архитектуре гнездовой постановочно-перестановочной сети (nested SPN), с блоками подстановки (S-боксами) размером 16x16 бит в оптико-электронных системах. В качестве факторов эффективности выбраны скорость преобразования в оптико-электронной системе и криптографическая стойкость двух последовательных слоев гнездовых подстановочно-перестановочных сетей разного типа.

Abstract. This note contains determine characteristics of effectiveness for block cipher in opto-electronic system. This cipher use a nested substitution-permutation networks as architecture. The size of S-box is 16x16 bites. A cryptographic security and a rate of transformation are factors of effectiveness in opto-electronic system. The effectiveness of ciphering is determined for two layers of nested substitution-permutation networks.

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

ВСТУП

Проблема підвищення ефективності шифрування в оптико-електронних системах є актуальною проблемою по причині постійного збільшення обсягу передавання інформації оптико-електронними системами та спроб несанкціонованого доступу до них.

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 повільною швидкістю перетворення інформації обчислювальними системами. Тенденції розвитку сучасних оптико-електронних систем демонструють збільшення швидкості передавання ними інформації в декілька раз. Тому існує доцільність визначити ефективність шифрування в оптико-електронних системах математичних 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-боксів розміром 16x16 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 16x16 біт. В роботі [5] визначені окремі показники стійкості блоків підстановки розміром 16x16 біт. Але в цих роботах відсутнє визначення показників ефективності шифрування в оптико-електронних системах.

Визначення показників ефективності шифрування в оптико-електронних 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 криптографічного перетворення, що виконується гніздовою SPN-мережею довжиною 128 біт з S-боксами розміром 16x16 біт в оптико-електронних системах з 64-ох бітними процесорами.

ПОСТАНОВКА ЗАВДАННЯ

Для визначення ефективності шифрування в оптико-електронних системах підстановочно-перестановочних мереж слід визначити коефіцієнт, який буде пов`язувати криптографічні показники з часом, який необхідно витратити, на виконання цього перетворення. Найважливішим криптографічним показником є стійкість до певного типу криптаналізу. Найпотужнішими типами криптаналізу є лінійний та диференційний. Тому доцільно визначити саме стійкість гніздової SPN-мережі з S-боксами розміром 16x16 до цих типів криптаналізу. Час, який слід витратити, на обчислювальне перетворення залежить від швидкості реалізації цього перетвореня в оптико-електронній системі. Перетворення, що відбувається на верхньому та нижньому рівнях, гніздової SPN-мережі містять операції, що вимагають різну кількість тактів процесора, який є складовою оптико-електронної системи. Ефективність шифрування гніздових SPN в оптико-електронних системах має бути компромісним варіантом від стійкості гніздової SPN-мережі та швидкості її реалізації в оптико-електронній системі. Для загального способу реалізації SPN-мережі в різних оптико-електронних системах 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 криптаналізу. На другому кроці визначимо кількість табличних підстановок та коефіцієнти ефективності шифрування двох рівнів SPN-мереж з S-боксами розміром 16x16 біт в оптико-електронних системах.

РОЗВ`ЯЗАННЯ

Криптографічна стійкість перетворення до лінійного та диференційного криптаналізу 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 - $КМВ_н$ та $КМВ_в$. Для SPN-мережі такого типу кількість активних S – боксів дорівнює

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

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

Код КМВ (2*m*, *m*, *m*+1) – код з твірною матрицею $G = [I] \cdot [C]$, де *C* – твірна матриця розміром *m* x *m*, *I* – одинична матриця, *m* – довжина слова кода. 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:

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

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

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 х 16. В таблиці 1 наведені можливі типи гніздових SPN-мереж довжиною 128 біт з S-боксами розміром 16 х 16 та відповідна кількість активних S-боксів.

Таблиця 1.

Варіанти гніздових SPN-мереж з S-боксами розміром 16х16 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 таблиці 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 *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* х *n* визначається виразом:

$$q_s = p_s = \frac{n}{2^{n-1}}, \tag{6}$$

де n – розмір S-боксу.

З виразу (6) випливає, що для S-боксів розміром 16 х 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 таблиці 2.

Таблиця 2.

Варіанти гніздових SPN-мереж з S-боксами розміром 16х16 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:

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

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

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

А результат одного рівня визначається виразом :

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

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 порядка поля – n та довжини слова КМВ – m.

Операції табличних підстановок – це операції читання даних з пам`яті процесора оптико-електронної системи. Кількість операцій читання даних визначається виразом:

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

де d – довжина даних (біт); w – довжина слова процесора (біт).

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

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

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

$$k = d*m/w = m_н{}^2 n/w + m_в{}^2 n/w, \quad (12)$$

де $m_н$ – довжина слова коду з максимальною відстанню на нижньому рівні гніздової SPN мережі; $m_в$ – довжина слова коду з максимальною відстанню на верхньому рівні гніздової SPN мережі.

В таблиці 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 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 3 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 16х16 біт в оптико-електронних системах, що містять процесор 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 16х16 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 8х8 в 64-ох бітних системах становлять 4,68-6,4[6]. Тоді реалізація SPN-мереж з S-боксами розміром 16х16 біт збільшує показники ефективності в 2,4-3,2 рази по зрівнянню з гніздовими SPN мережами, що використовують S-бокси розміром 8х8 біт.

ВИСНОВКИ

В ході проведенного дослідження визначено показники ефективності реалізації двох рівнів гніздових SPN-мереж довжиною 128 біт та розміром S-боксів 16х16 біт в оптико-електронних системах. Отримані чисельні значення коефіцієнтів ефективності демонструють, що застосування в гніздовій SPN-мережі S-боксів розміром 16х16 біт підвищить ефективність реалізації в оптико-електронній системі по відношенню до SPN-мережі з S-боксами розміром 8х8 біт приблизно в 2,4-3,2 рази. В якості подальших досліджень необхідно визначити тип математичних перетворення, що мають відбуватися S-боксами та показники ефективності реалізації перетворення з певною кількістю раундів в оптико-електронних 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 /[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 / Ростовцев А. // Проблемы информационной безопасности. Компьютерные системы . - 2000. - № 3. – С. 31–35
6. 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.
7. 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.
8. Chen S., Shu R. Block permutation cipher in Chaos with feistel structure for wireless sensor networks / Chen S., Shu R. / [Електронний ресурс].– Режим доступу World Wide Web: www.scopus.com/results/results.url?sort=plf-f&src=s&st1=block+cipher&sid=RwJFNbhqR-InD0ViHtCa0Nb%3a30&sot=b&sdt=b&sl=27&s=TITLE-ABS-KEY(block+cipher)&origin=searchbasic&txGid=RwJFNbhqR-InD0ViHtCa0Nb%3a3

9. Ortega J. Parallelizing AES on multicores and GPUs / J. Ortega, H. Trefftz, C. Trefftz / [Електронний ресурс].– Режим доступу World Wide Web: http://www.scopus.com/record/display.url?eid=2-s2.0-80155132472&origin=resultslist&sort=plf-f&src=s&st1=block+cipher&sid=RwJFNbhqR-InD0ViHtCa0Nb%3a70&sot=b&sdt=b&sl=27&s=TITLE-ABS-KEY%28block+cipher%29&relpos=3&relpos=3&searchTerm=TITLE-ABS-KEY(block%20cipher)

Надійшла до редакції 21.11.2011р.

БЕВЗ О.М. – кандидат технічних наук, доцент кафедри АІВТ, Вінницький національний технічний університет, м.Вінниця, Україна

ПАПІНОВ В.М. – кандидат технічних наук, доцент кафедри АІВТ, Вінницький національний технічний університет, м.Вінниця, Україна