УДК 681.3.06

Рябов О.Д.
Бевз О.М.
Барабан М.В.

МЕТОДИ ШИФРУВАННЯ НА ОСНОВІ БАГАТОРІВНЕВИХ ПІДСТАНОВЧНО-ПЕРЕСТАНОВОЧНИХ МЕРЕЖ

Вінницький національний технічний університет

Анотація
В статті проведено дослідження, мета якого визначення стійкості блочних шифрів, довжина блоку яких складає 256 та 512 біт.
Ключові слова: гніздова підстановочно-перестановочна мережа, криптоаналіз, блочні шифри, лінійне перетворення, код з максимальною відстанню (КМВ).

Abstract
In this article, the purpose of which is to determine the stability of block ciphers, the block length of which is 256 and 512 bits.
Keywords: nested substitution- permutation network, cryptanalysis, block ciphers, linear transformation, Maximum Distance Separable (MDS).

Актуальність

Стрімкий розвиток сучасних технологій комп'ютерних систем та мереж слугує розвитку широкого діапазону новітніх інформаційних сервісів та служб, які, в свою чергу, інтегруються в багатофункціональні обчислювальні мережі. Однією з головних задач по забезпеченню конфіденційності, цілісності та автентичності передачі даних є захист інформації від несанкціонованого доступу. На сьогодні мільярди людей пов'язані між собою за допомогою комп'ютерних систем та мереж глобальною мережею Internet. Служби мережі Internet, такі як: електронна пошта (E-mail) , Інтернет-банкінг, медичні бази даних, електронна комерція – базуються та вимагають захисту приватного характеру інформації та інтересів споживачів. Наприклад, для трансакцій з платіжними картками в Інтернет-магазині, продавець вимагає номер платіжної карти. Якщо дане з'єднання не закрите, зловмисники з легкістю можуть отримати доступ до конфіденційних даних. Тому реалії сучасного життя спонукають до активної розробки та вдосконалення різноманітних методів для захисту інформації.

На сьогоднішній день захист інформації здійснюється за допомогою та на основі сучасних техніко-економічних криптографічних засобів. Перевіреним способом захисту даних є використання блочних шифрів, тому формування блочних шифрів з високою криптографічною стійкість є актуальною задачею.

Визначення кількості активних S-боксів в SPN мережі, довжина блоку яких складає 256 та 512 біт

Сучасні блочні шифри – ітераційні шифри. Кожна ітерація представляє собою раундове перетворення. Одним з варіантів реалізації раундового перетворення є застосування кодів з максимальною відстанню (КМВ). Для формування ефективного методу раундового перетворення необхідно визначити тип КМВ-перетворення. Тип КМВ перетворення впливає на максимальну протидію лінійному та диференціального криптоаналізу. [1] Показник протидії криптоаналізу – кількість необхідної інформації. Кількість необхідної інформації (стійкість) ε для успішного проведення диференційного або лінійного криптаналізу приблизно визначається виразом:

$$\varepsilon \approx \log_2 1/\mathrm{P}, \tag{1}$$

де P – ймовірність лінійної оболонки або диференціальної характеристики.

Як визначено вище, ймовірність лінійної оболонки або диференціальної характеристики P залежить від кількості активних S-боксів. Кількість активних S-боксів на кожному рівні гніздової SPN визначається коефіцієнтом розсіювання перетворення, яке залежить від типу КМВ. Поширеним варіантом реалізації лінійного перетворення є перетворення, яке складається з двох рівнів: верхнього та нижнього. Таке перетворення має назву гніздова підстановочно-перестановочна мережа (Nested SPN).

Так для прикладу в чотирьох раундах гніздової SPN верхній рівень буде містити m1+1 активних S-боксів в тому випадку, якщо він реалізований КМВ. Показник m1 – це довжина слова КМВ. В свою чергу на верхньому рівні в такому випадку кількість активних S-боксів дорівнює m2+ 1. Тому сукупна кількість активних S-боксів низького рівня дорівнює (m2+ 1)(m1 + 1) [2, 3].

В дослідженні визначена кількість активних S-боксів для гніздової SPN-мережі з розміром S-боксу 8 біт при довжині блоку шифрування 256 та 512 біт. В таблиці 1 наведені варіанти гніздових SPN, тип КМВ-кодів для реалізації лінійного перетворення верхнього та нижнього рівнів, та відповідна кількість активних S-боксів, що створюються послідовністю чотирьох раундів для S-боксів розміром 8 біт довжиною SPN-мережі 256 біт.

Таблиця 1. Варіанти гніздових SPN-мереж з S-боксами розміром 8 біт та відповідна кількість активних S-боксів для довжини блоку 256 біт

Номер варіанта	Тип КМВ нижнього рівня	Тип КМВ верхнього рівня	Кількість активних S-боксів
1	(2,1,2)	(64, 32, 33)	66
2	(4, 2, 3)	(32, 16, 17)	51
3	(8, 4, 5)	(16,8,9)	45
4	(16,8,9)	(8,4,5)	45
5	(32, 16, 17)	(4, 2, 3)	51
6	(64, 32, 33)	(2,1,2)	66

Аналогічно розрахуємо кількість активних S-боксів, що необхідна для довжини блоку 512 біт. Результати розрахунків та можливі варіанти архітектури мереж наведені в таблиці 2.

Таблиця 2. Варіанти гніздових SPN-мереж з S-боксами розміром 8 біт та відповідна кількість активних S-боксів для довжини блоку 512 біт.

Номер варіанта	Тип КМВ нижнього рівня	Тип КМВ верхнього рівня	Кількість активних S-боксів
1	(2,1,2)	(256,128,129)	258
2	(4,2,3)	(128,64,65	195
3	(8,4,5)	(64,32,33)	165
4	(16,8,9)	(32,16,17)	153
5	(32,16,17)	(16,8,9)	153
6	(64,32,33)	(8,4,5)	165
7	(128,64,65)	(4,2,3)	195
8	(256,128,129)	(2,1,2)	258

Визначення криптографічної стійкості лінійного перетворення на основі КМВ-коду для довжини блоку 256 та 512 біт

Крім кількості активних S-боксів раунду, стійкість раундового перетворення залежить від значення ймовірності лінійної оболонки q та диференційної характеристики p. Як визначено вище криптографічну стійкість відносно до лінійного та диференціального криптоаналізу слід визначити кількістю інформації, що необхідна для проведення результативного аналізу.

Кількість інформації обернено пропорційна верхній межі ймовірності диференційної характеристики або лінійної оболонки.

Для S-боксів розміром 8 біт верхня межа ймовірності лінійної оболонки q_s дорівнює верхній межі ймовірності диференційної характеристики p_s і дорівнює 2^{-6}. [4]

Зведемо ці дві межі ймовірності до однієї межі P:

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

Використовуючи вираз (2), визначимо верхню межу ймовірності лінійної оболонки та диференційної характеристики та стійкість для раундового перетворення, що складається з гніздової

SPN з різними типами КМВ-перетворення. В таблиці 3 наведено варіанти гніздових SPN-мереж та ймовірності лінійної та диференціальної характеристики із значенням стійкості для довжини блоку 256 біт.

Таблиця 3. Варіанти гніздових SPN-мереж з S-боксами розміром 8 біт та відповідне значення ймовірності лінійної та диференціальної характеристики і стійкості для довжини блоку 256 біт

Номер варіанта	Кількість активних S-боксів	Значення ймовірності	Стійкість
1	66	2^{-396}	396
2	51	2^{-306}	306
3	45	2^{-270}	270
4	45	2^{-270}	270
5	51	2^{-306}	306
6	66	2^{-396}	396

Відповідно до виконаних вище дій, занесемо до таблиці 4 варіанти гніздових SPN-мереж та ймовірності лінійної та диференціальної характеристики із значенням стійкості для довжини блоку 512 біт.

Таблиця 4. Варіанти гніздових SPN-мереж з S-боксами розміром 8 біт та відповідне значення ймовірності лінійної та диференціальної характеристики і стійкості для довжини блоку 512 біт

Номер варіанта	Кількість активних S-боксів	Значення ймовірності	Стійкість
1	258	2^{-1548}	1548
2	195	2^{-1170}	1170
3	165	2^{-990}	990
4	153	2^{-918}	918
5	153	2^{-918}	918
6	165	2^{-990}	990
7	195	2^{-1170}	1170
8	258	2^{-1548}	1548

Висновки

В ході проведеного дослідження було визначено криптографічну стійкість для блочного шифру з довжиною блоку 256 та 512 біт, лінійне перетворення якого складається з гніздових мереж різного типу та визначено тип кодів з максимальною відстанню, який буде реалізовувати максимальну протидію лінійному та диференційному криптоаналізу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kaliski B. On differential and linear cryptanalysis of RC5 / Kaliski B., Yin Y. // Advanced in Cryptology - Crypto'95, Lecture Notes in Computer Science. - Springer-Verlag. - 1995. -Vol. 963. -P.171-184.
2. Knudsen L. Practical secure Feistel ciphers / Knudsen L. // Fast Software Encryption, Lecture Notes in Computer Science - Springer-Verlag. -1994.-Vol. 809.-P.211-221.
3. Kocher P. Differential Power Analysis / Kocher P., Jaffe J., and Jim B // Proceedings of Cryptox99. - Advances in Cryptology, Lecture Notes in Computer Science. - Springer-Verlag. - 1999. -Vol. 1666. -P.388-397.
4. Столлингс В. Криптография и защита сетей:принципы и практика. Столлингс В.- М.: Издательский дом "Вильяме", 2002. - 672 с.

Рябов Олексій Дмитрович, група 1АКІТ-17м, Факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, м. Вінниця. E-mail: worner2008@gmail.com

Бевз Олександр Миколайович, к.т.н., доц., доцент кафедри АІ ІТ, Вінницький національний технічний університет, м. Вінниця.

Барабан Марія Володимирівна, к.т.н., ст. викл. кафедри АІ ІТ, Вінницький національний технічний університет, м. Вінниця.

Ryabov Oleksii D., Faculty of Computer Systems and Automatics, Vinnitsa National Technical University, Vinnytsia. E-mail: worner2008@gmail.com

Bevz Oleksandr M., Ph.D., Associate Professor, Department of Automation and Intelligent Information Technologies, Vinnytsia National Technical University, Vinnytsia.

Baraban Mariya V., Ph.D., Senior Lecturer of the Department of AI IT, Vinnytsia National Technical University, Vinnytsia.