КРИПТОГРАФІЧНІ ВЛАСТИВОСТІ ПІДСТАНОВОЧНО-ПЕРЕСТАНОВОЧНИХ МЕРЕЖ

Бевз О. М.
Вінницький національний технічний університет
кафедра автоматики та інформаційно-вимірювальної техніки
E-mail:abevz@aime.vstu.vinnica.ua

Abstract
Bevz O. M. Cryptographic characteristics of the substitution-permutation network *In this article was investigated a differential characteristics of the substitution-permutation network and developed a upper bound of a probability differential characteristic.*

Вступ. Причини збільшення кількості спроб несанкціонованого доступу до приватної інформації лежать в зростанні об`ємів передавання, обробки і зберігання інформації в сучасному інформаційному світі, існування великої кількості користувачів обчислювальних систем і мереж. Один з способів захисту інформації від несанкціонованого доступу — шифрування інформації по певним алгоритмам з застосуванням ключа, який визначає ступінь секретності. Сучасні шифри складаються з певною кількості однорідних процедур — раундів і базуються на принципах введених Шенноном [1]. Ці принципи ґрунтуються на поняттях “перемішування” та “розсіювання”. Частина шифру, що виконує “перемішування” має назву S-бокс. Частина шифру, що виконує “розсіювання” і визначає зв`язок між S-боксами має назву мережа. Архітектура шифру визначається типом мережі, що використовує шифр. Однією з поширених типів мереж є підстановочно-перестановочна мережа [2] рисунок 1.

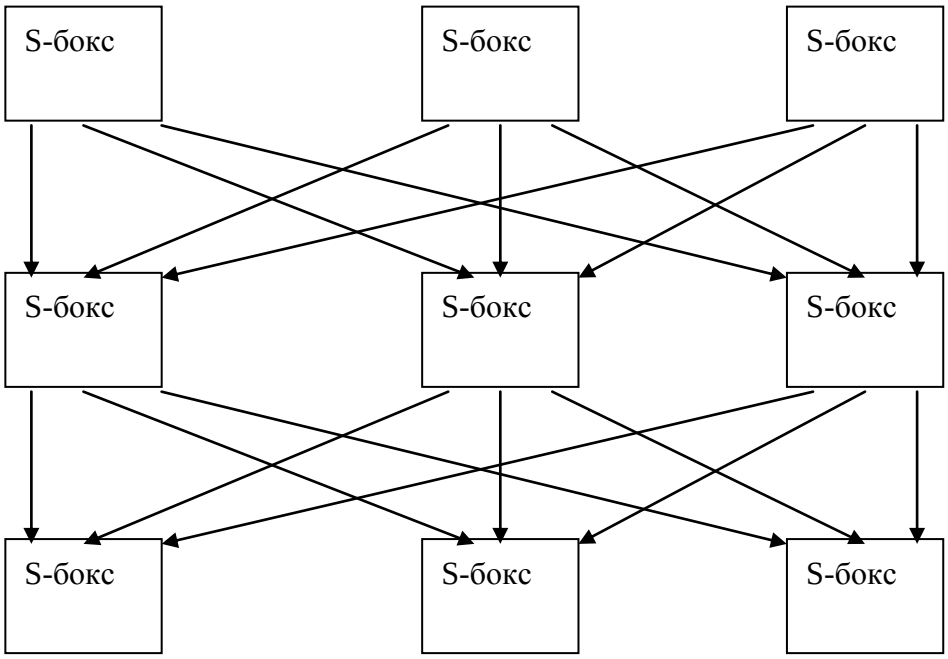

Рисунок 1 — Підстановочно-перестановочна мережа

Головна криптаналітична властивість шифру — стійкість. Стійкість — це здатність шифру протидіяти певному криптаналізу. Одним з видів криптаналізу, що успішно визначає біти ключа, є диференційний криптаналіз [3]. Процедура визначення факторів та умов, які впливають на стійкість шифрів з архітектурою підстановочно-перестановочної мережі відносно диференційного криптаналізу дасть можливість проектувати криптографічні системи з великим ступенем протидії до цього аналізу.

Мета цієї статті — визначення факторів, які впливають на стійкість шифрів з підстановочно-перестановочною мережею та визначення верхньої межі показника стійкості.

Напрямок та задачі дослідження**.** Результативність диференційного аналізу визначається кількістю пар відкритий текст — шифртекст. Якщо це значення менше за кількість варіантів перебору всіх можливих ключів, то шифр вважається вразливим до криптаналізу. Кількість пар шифртекстів, необхідних для реалізації цього аналізу, визначається виразом (1) [4]

$$N = 1/p_{max}, \quad (1)$$

де p_{max} — верхня межа ймовірності існування кортежу диференціалів відкритий текст-шифртекст (характеристики).

Тому визначення факторів впливу на стійкість слід проводити в напрямку визначення чинників, що створюють верхню межу існування характеристики.

Задачею дослідження є визначення критичних факторів та складових частин шифрування, що створюють верхню межу існування характеристики та встановлення математичного зв`язку між ними.

Результати дослідження. Для виконання задачі дослідження, що поставлена в статті, необхідно дослідити механізм роботи диференційного криптаналіза на підстановочно-перестановочні мережі. Як вже було наведено вище диференційний криптаналіз — засіб для встановлення бітів ключа, що використовує пари відкритий-закритий текст з певними відмінностями.

Так цей аналіз перевіряє зміни шифртексту при певних змінах відкритого тексту. Зміни відкритого та закритого текстів мають назви диференціали — ΔP і в термінах цього аналізу визначаються як результат операції додавання за модулем 2 між окремими парами відкритих або закритих текстів вираз (2):

$$\Delta P = P_1 \oplus P_2. \quad (2)$$

Цей криптаналіз оснований на існуванні високоймовірних характеристик. Де r — раундова характеристика Ch_r, визначається як послідовність диференціальних пар $Ch_r=[(\Delta X_1\ \Delta Y_1)\ ...\ (\Delta X_r\ \Delta Y_r)]$. Криптаналіз використовує вхідні пари з певними відмінностями і підраховує кількість раз, коли підключ відповідає значенню шифртексту. Якщо характеристика виникає з ймовірністю *p*, вірні біти підключа визначаються з ймовірністю меншою за *p*. Після відповідної кількості перевірок вірний підключ буде виникати значно частіше.

Ймовірність характеристики визначається добутком ймовірності виникнення одноразундових диференційних пар (3).

$$p_r=\Pi\ P(\Delta X_i\ \Delta Y_i), \quad (3)$$

де ΔX_i — диференціал вхідних бітів раунду *i*;

ΔY_i — диференціал вихідних бітів раунду *i*;

P — ймовірність, що диференціал входу ΔX_i створить диференціал виходу ΔY_i.

Вираз (3) дає ймовірність характеристики, визначеної незалежним розподіленням відкритих текстів та ключів.

Диференційний криптаналіз підстановочно-перестановочних мереж виконується аналогічно диференційному криптаналізу на мережу Фейстеля. Для мережі Фейстеля диференційний криптаналіз визначає біти ключа, що використовуються на останьому раунді шифрування. Ця процедура використовує значення двох вхідних значень, які прямо доступні з правої частини шифртексту і їх диференціалів в останньому раунді функції з ймовірним знанням вихідного диференціалу останнього раунду.

Аналогічно, диференційний криптаналіз підстановочно-перестановочних мереж може бути використаний для визначення бітів ключа на виході останнього раунду S-боксу шляхом використання двох шифртекстів їх диференціалів і ймовірної інформації вхідного диференціалу в останій раунд S-боксу.

Диференційний криптаналіз підстановочно-перестановочних мереж може бути результативним, якщо існує високоймовірна характеристика для всіх раундів крім останього. Криптаналіз використовує S-бокс раунду R, який впливає на вихідні зміни характеристики. Визначений таким чином підключ містить біти ключа, що просумовані за модулем два з виходом S-боксу. Відповідно перевіряючи всі значення підключів, можливо використовувати відомий шифртекст для дешифрування частини раунду R, в якому знаходиться визначений вище S-бокс.

Якщо диференціал входу S-боксу визначений частковим дешифруванням відповідає справжньому значенню, то частота виникнення відповідного підключа збільшується на одиницю. Правильний підключ визначається як ключ, що має більшу частоту виникнення ніж інші ключі.

Нехай ΔX та ΔY — вхідні та вихідні диференціали окремого S-боксу. Існування високоймовірної характеристики залежить від двох факторів: розподілення диференційних пар $(\Delta X \quad \Delta Y)$, та поширення бітових змін через підстановочно-перестановочну мережу. Так мале поширення бітових змін приводить до великого значення ймовірності характеристики, тому що включає малу кількість S-боксів. Розглянемо для прикладу чотирьохраундну характеристику для підстановочно-перестановочної мержі з S-боксами, що мають 4 входи та 4 виходи та максимальною ймовірністю виникнення диференціалу $p = 0{,}25$. Нехай характеристика існує лише в одному S-боксі і вхідна зміна одного біта приводить до одної зміни вихідного біта в усіх раундах (рисунок 2).

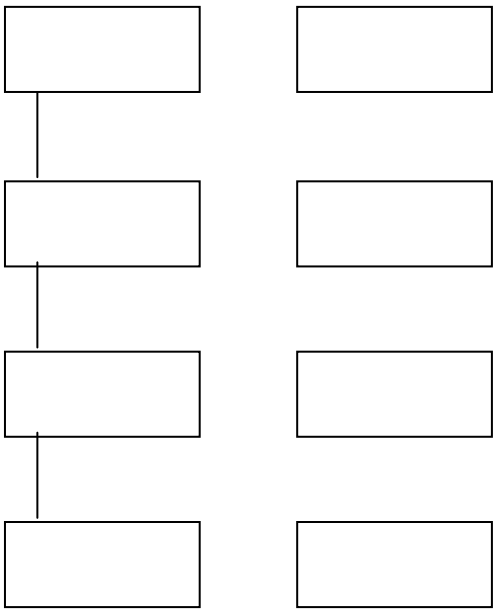

Рисунок 2 — Підстановочна-перестановочна мережа. Варіант 1

Така характеристика включає малу кількість S-боксів, очевидно, що ймовірність p такої чотирьохраундної характеристики обмежено значенням $0{,}25^4$.

В іншому випадку нехай всі S-бокси такі, що при зміні одного вхідного біта повинно змінюватися не менше двох вихідних бітів і що кожний S-бокс з попереднього раунду з`єднаний з двома S-боксами наступного раунду (рисунок 3).

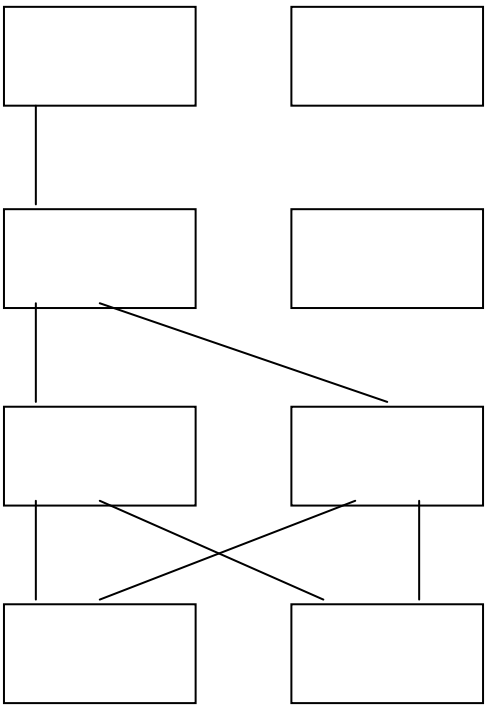

Рисунок 3 — Підстановочно-перестановочна мережа. Варіант 2

В цьому випадку характеристика проходить через шість S-боксів і значення її ймовірності обмежено $0{,}25^6$, що значно менше за попереднє.

Для визначення чинників впливу на створення характеристики введемо мінімальну сумарну вагу Хемінга диференціала входу-виходу: $z=w(\Delta X)+w(\Delta Y)$.

Розглянемо довільний S-бокс в довільно вибраному раунді R. Припустимо, що при зміні вхідних біт b_x кількість вихідних біт, що змінилися — b_y. Кількість S-боксів попереднього раунду R–1, що вплинули на кількість змінних біт b_x, в наслідок геометричних властивостей SPN-мережі буде також b_x. Кількість S-боксів, що змінять свої вихідні значення в раунді R+1 буде b_y.

В межах одного S-боксу $b_x = w(\Delta X)$, $b_y = w(\Delta Y)$. Тоді N мінімальна кількість S-боксів, що задіяні в створені диференціалу $(\Delta X; \Delta Y)$ буде $N = b_x + b_y + 1 = w(\Delta X)+w(\Delta Y) + 1 = z + 1$.

Визначимо верхню межу ймовірності трьохраундової характеристики.

Нехай p_{max} — максимальна ймовірність виникнення диференціалу $(\Delta X; \Delta Y)$ в S-боксі. “Рух” цього диференціалу через три раунди R–1 $\Rightarrow$ R $\Rightarrow$ R+1 — “рух” через певні S-бокси. Ймовірність трьохраундової характеристики буде приймати максимальне значення, коли кількість S-боксів через які “рухається” диференціал $(\Delta X; \Delta Y)$ буде мінімальною і буде дорівнювати $z + 1$. Підсумовуючи вищенаведене верхня межа p_{sup} ймовірності трьохраундової характеристики визначається виразом (4)

$$p_{sup} = (p_{max})^{z+1} = (p_{max})^{w(\Delta X)+w(\Delta Y)+1}. \quad (4)$$

Верхня межа ймовірності характеристики кількості раундів R, що кратні 3 буде відповідно визначатися виразом (5):

$$p_{sup} = (p_{max})^{(z+1)R/3} = (p_{max})^{(w(\Delta X)+w(\Delta Y)+1)R/3}. \quad (5)$$

Верхня межа ймовірності характеристики кількості раундів R=3n+1, де n≥1, визначається виразом (6):

$$p_{sup} = (p_{max})^{(z+1)R/3+1} = (p_{max})^{(w(\Delta X)+w(\Delta Y)+1)R/3+1}. \quad (6)$$

Верхня межа ймовірності характеристики кількості раундів R=3n+2, де n≥1 відповідає виразу (4):

$$p_{sup} = (p_{max})^{(z+1)R/3+2} = (p_{max})^{(w(\Delta X)+w(\Delta Y)+1)R/3+2}. \quad (7)$$

З виразів (5) – (7) очевидно, що верхня межа ймовірності характеристики залежить прямо пропорційно від кількості раундів та мінімальної сумарної ваги Хемінга диференціалу входу виходу окремого S-боксу.

Використання S-боксів з великим значенням мінімальної сумарної ваги Хемінга диференціалів експоненціально зменшує верхню межу всієї характеристики і тим самим збільшує протидію диференційному криптаналізу.

Крім того використання таких S-боксів зменшує кількість раундів шифрування, що приводить до підвищення швидкості шифрування.

Підстановочно-перестановочна мережа, в якій кожний вихід кожного S-боксу з`єднаний з входами кожного S-боксу наступного раунду має мінімальне значення верхньої межі ймовірності характеристики по зрівнянню з підстановочно-перестановочними мережами з такою самою кількістю раундів та S-боксів.

Висновки. Шляхом введення мінімальної сумарної ваги Хемінга диференціалу входу-виходу визначено верхню межу ймовірності виникнення характеристики для будь-якої кількості раундів шифрування та фактори, які на неї впливають. Стійкість шифру до диференційного криптаналізу залежить від типу підстановочної мережі, диференціальних характеристик S-боксів та кількості раундів. Врахування цих факторів приведе до створення шифрів з високою стійкістю до диференційного криптаналізу. Зменшення раундів шифрування при збережені стійкості можна виконувати застосуванням S-боксів з великою мінімальною сумарною вагою Хемінга диференціалів входу виходу, що в сукупності дасть можливість підвищити швидкості шифрування.

Література

1. К. Шеннон. Теория связи в секретных системах. — М.: Связь, 1978. — 40 с.
2. A. Shimizu and S. Miyaguchi. Fast data encripherment algorithm: FEAL. Advanced in Cryptology: Proceedings of Eurocrypt`87, Springer-Verlag, Berlin, 1988. — P. 267–278.
3. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 1991, 4(1). — P. 3–72.
4. E. Biham and A. Shamir. Differential cryptanalysis of the full 16-round DES. Advanced in Cryptology: Proceedings of Crypto’ 92, Springer-Verlag, 1993. — P. 487–496.