Вінницький національний технічний університет

Методи шифрування на основі багаторівневих підстановочно-перестановочних мереж

Доповідач: студент групи 1АКІТ-17м, *Рябов О.Д.*
Науковий керівник: к.т.н., доц. *Бевз О.М.*

Вступ

- ***Метою роботи*** є підвищення стійкості захисту інформації в комп'ютерних системах та мережах на основі розробки нових методів формування блочних шифрів і засобів шифрування.
- ***Об'єкт дослідження*** – процес перетворення даних для захисту інформації в комп'ютерних системах і мережах.
- ***Предмет дослідження*** – методи шифрування для захисту інформації в комп'ютерних системах та мережах.
- ***Наукова новизна:*** отримав подальший розвиток метод формування лінійного рівня блочних шифрів, який на відміну від існуючих використовує багаторівневі підстановочно-перестановочні мережі в основі яких лежать коди з максимальною відстанню для шифрів з довжиною блоку 256 та 512 біт, що дає можливість підвищити криптографічну стійкість за рахунок збільшення кількості активних S-боксів.

Актуальність

Сфери застосування:

- Електронна пошта;
- Інтернет-банкінг;
- Бази даних;
- Електронна комерція;

Види загроз:

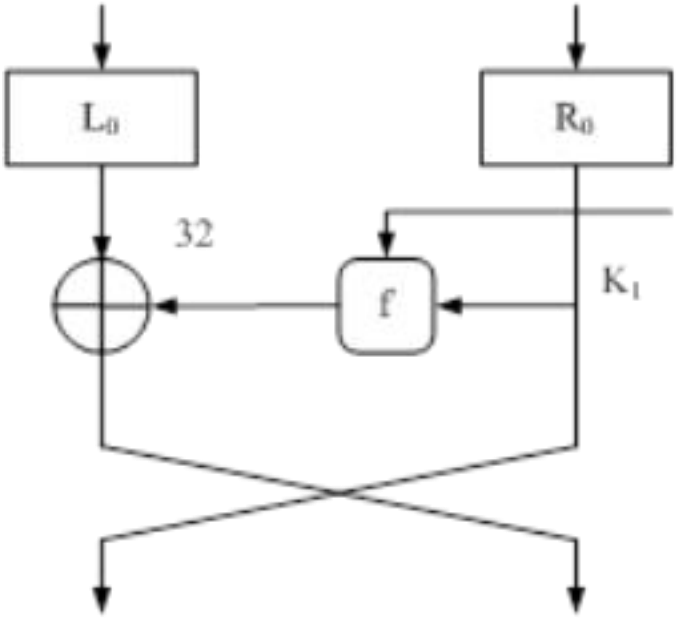
- перехоплення даних;
- модифікація чи переадресація;
- несанкціонована відправка даних від імені інших користувачів;
- невідповідність автентичності даних;
- факти відправлення або отримання інформації;

Класифікація сучасних методів блочного шифрування

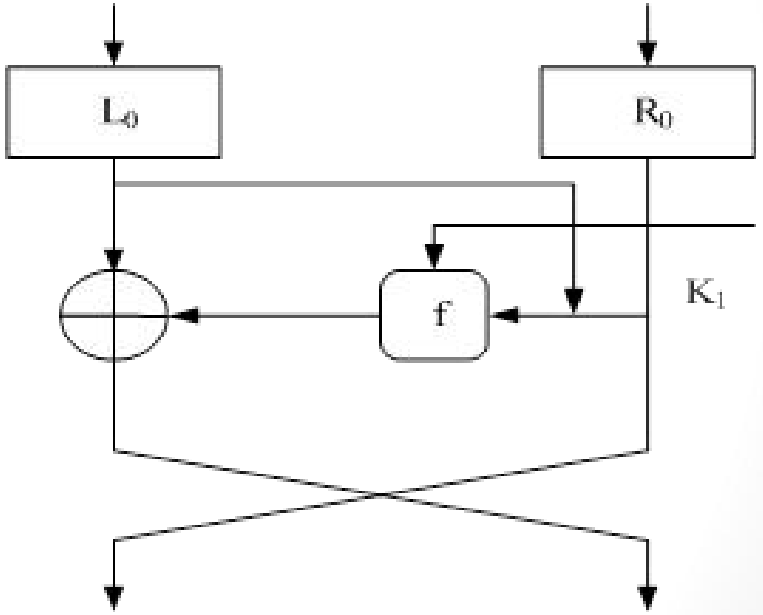
- Мережа Фейстеля;
- Substitution-Permutation Network (SPN);

Мережа Фейстеля

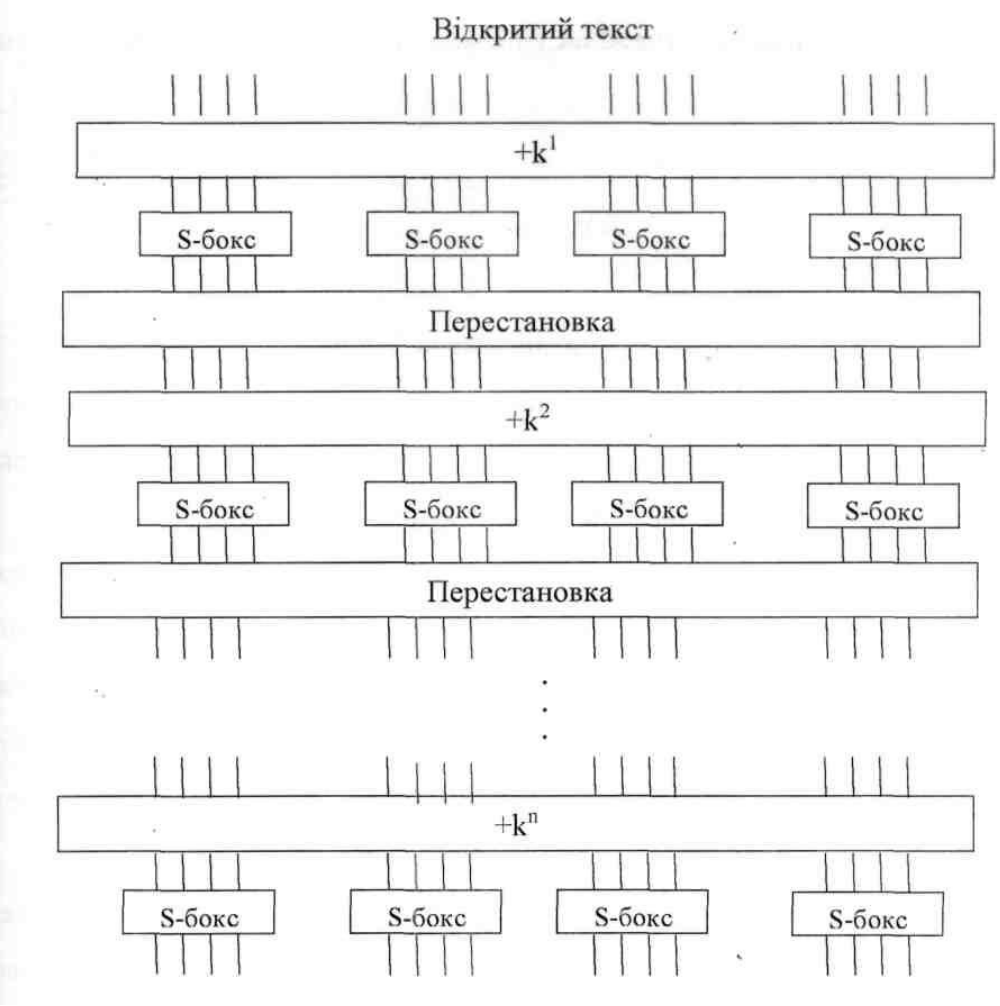
Збалансована мережа



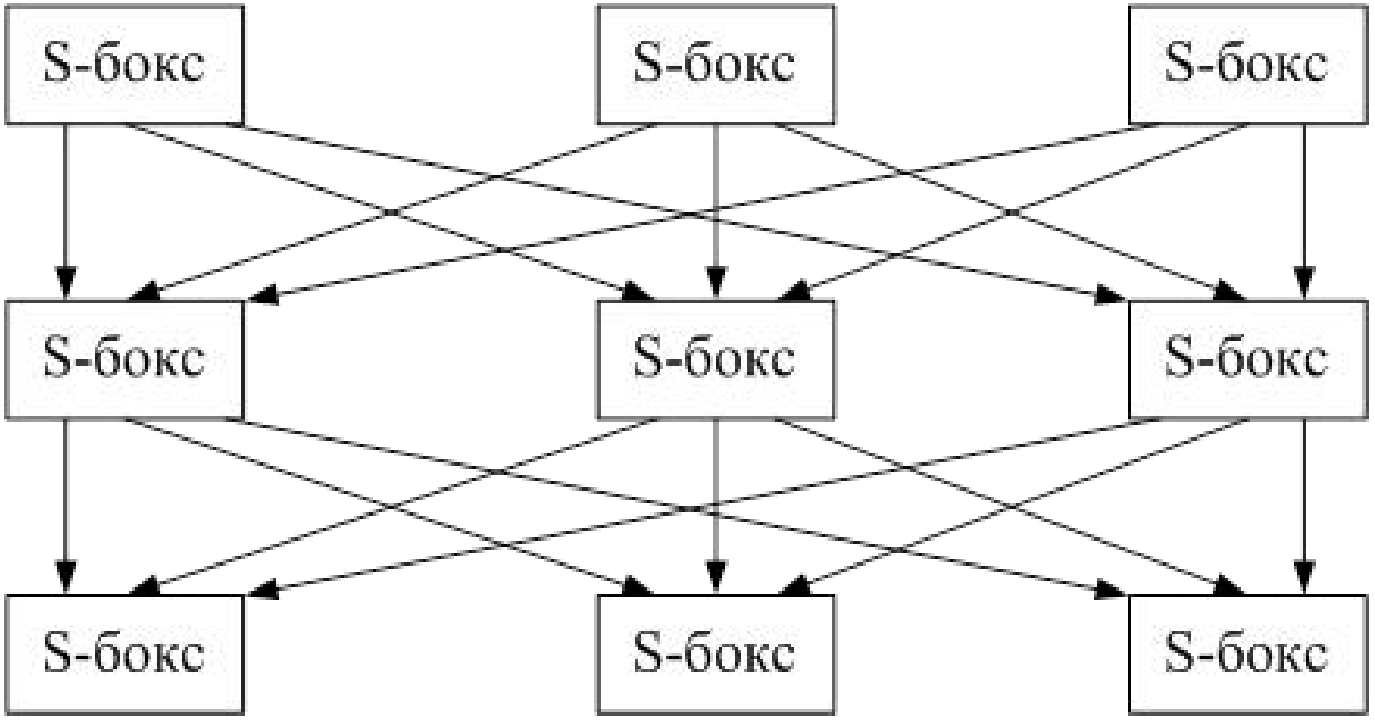
Незбалансована мережа



Substitution-Permutation Network



Приклад SPN-мережі, що складається з трьох раундів

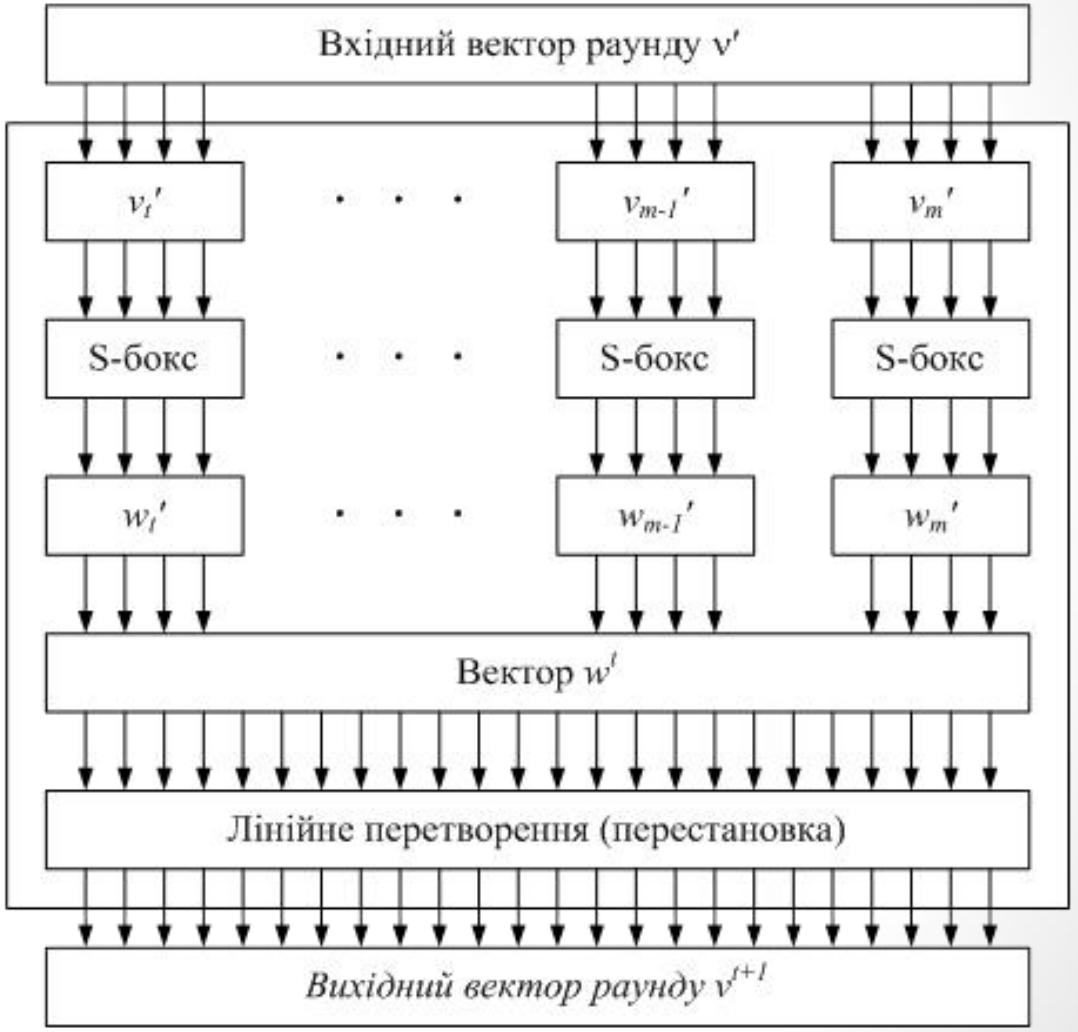


Лінійне перетворення

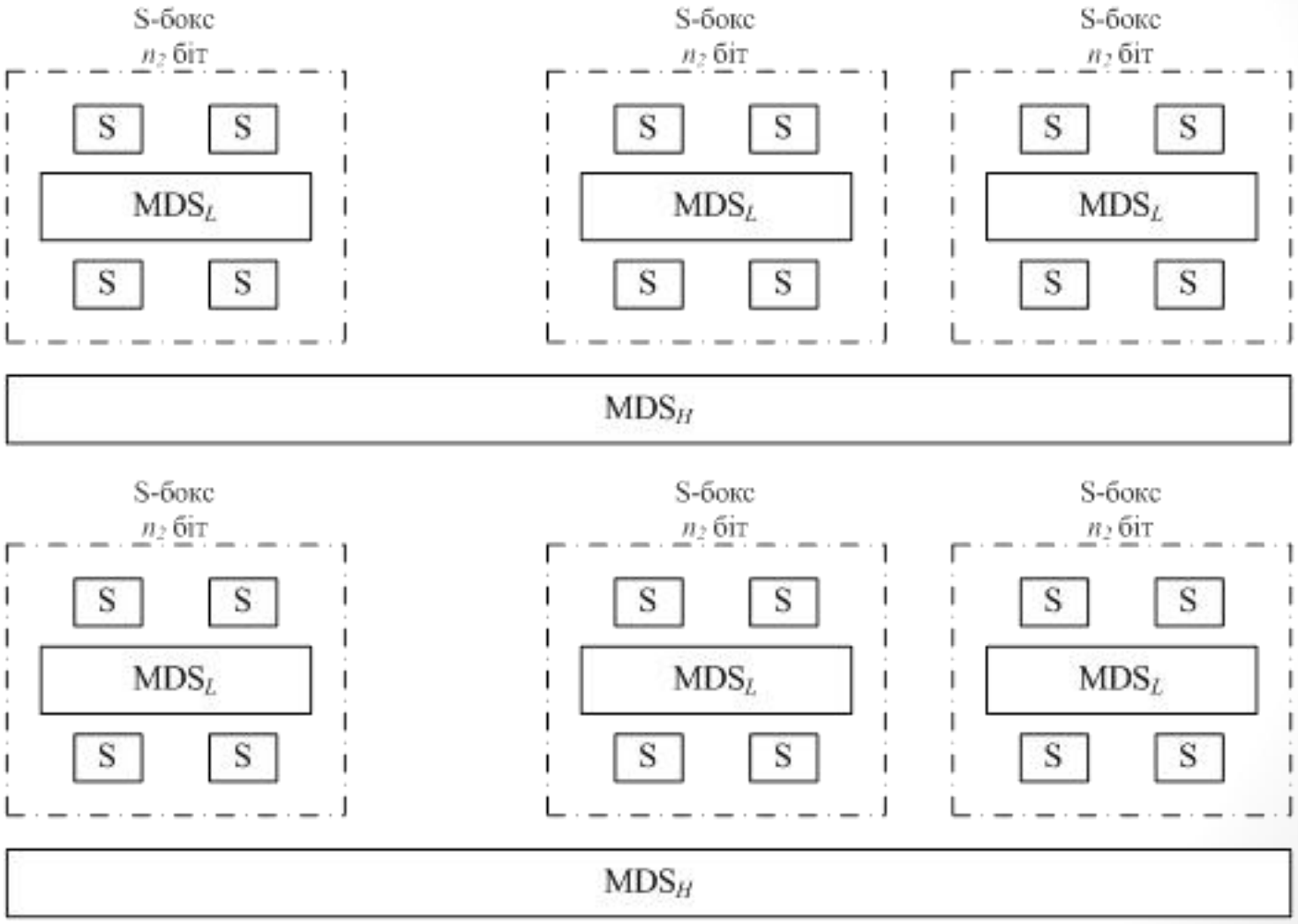
$$a = \chi b \qquad (1)$$

$$\nu a = w(\chi b) \quad (2)$$

$$\nu = \chi' \qquad (3)$$



Гніздові SPN



Математичне представлення перетворення, що здійснюється Кодом з Максимально Відстанню (КМВ)

- $B = FA,$ (4)

де $B = \begin{pmatrix} b_0 \\ \vdots \\ b_{m-1} \end{pmatrix}, A = \begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \end{pmatrix}, F = \begin{pmatrix} f_{n-1,n-1} & \cdots & f_{n-1,0} \\ \vdots & \vdots & \vdots \\ f_{0,n-1} & \cdots & f_{0,0} \end{pmatrix}$

- $f_{n-1,j}x^{n-1}+\ldots+f_{0,j} = x^j(c_{n-1}x^{n-1}+\ldots+c_0)\mathrm{mod}P(x)$ (5)

- Кожний елемент матриць *B*, *A*, *F* – елемент поля GF (2^n),
- *P(x)* – неподільний поліном в кінцевому полі.

Визначення стійкості

KMB(2m, m, m+1)

- $n = (m_2 + 1)(m_1 + 1)$ (6)
  - Сукупна кількість активних S-боксів
- $\varepsilon \approx \log_2 1/\mathrm{P}$ (7)
  - Криптографічна стійкість
- $P = p_s^n = q_s^n = (2^{-6})^n$ (8)
  - Значення ймовірності

Практичні результати

Таблиця 1

Номер варіанта	Тип КМВ нижнього рівня	Тип КМВ верхнього рівня	Кількість активних S-боксів	Значення ймовірності	Стійкість
1	(2,1,2)	(64, 32, 33)	66	2^{-396}	396
2	(4, 2, 3)	(32, 16, 17)	51	2^{-306}	306
3	(8, 4, 5)	(16,8,9)	45	2^{-270}	270
4	(16,8,9)	(8,4,5)	45	2^{-270}	270
5	(32, 16, 17)	(4, 2, 3)	51	2^{-306}	306
6	(64, 32, 33)	(2,1,2)	66	2^{-396}	396

Таблиця 2

Номер варіанта	Тип КМВ нижнього рівня	Тип КМВ верхнього рівня	Кількість активних S-боксів	Значення ймовірності	Стійкість
1	(2,1,2)	(128,64,65)	130	2^{-780}	780
2	(4,2,3)	(64,32,33)	99	2^{-594}	594
3	(8,4,5)	(32,16,17)	85	2^{-510}	510
4	(16,8,9)	(16,8,9)	81	2^{-486}	486
5	(32,16,17)	(8,4,5)	85	2^{-510}	510
6	(64,32,33)	(4,2,3)	99	2^{-594}	594
7	(128,64,65)	(2,1,2)	130	2^{-780}	780

Висновки

Таблиця 3 – Необхідний об’єм пам’яті для роботи алгоритмів шифрування

Назва алгоритму	Розмір ПЗП (Кбайт) для блоку 256 біт	Розмір ПЗП (Кбайт) для блоку 512 біт
Rijndael	1650	3300
Twofish	1600	3200
Mars	1588	3176
RC6	1632	3264
Запропонований Алгоритм	1504	3008

Таблиця 4 – Швидкість роботи алгоритмів шифрування

Назва алгоритму	Швидкість шифрування Гбіт/с для блоку 256 біт	Швидкість шифрування Гбіт/с для блоку 512 біт
Rijndael	2,66	5,32
Twofish	2,2	4,4
Mars	2,06	4,12
RC6	2,8	5,6
Запропонований Алгоритм	2,94	5,88

Дякую за увагу