Методи шифрування на основі високонелінійних бульових функцій з використанням паралельних обчислень

Студент гр. 1АКІТ-17м
Кримчук Богдан

Керівник к.т.н., доц.
кафедри АІІТ Бевз О.М.

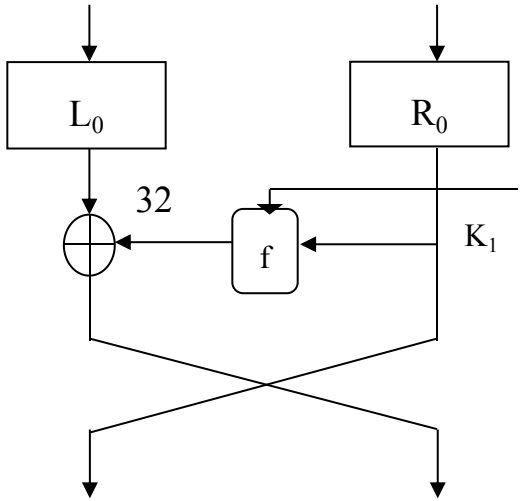
Мета: підвищення швидкості реалізації захисту інформації в комп'ютерних системах та мережах на основі розробки нових методів та засобів паралельного обчислення результатів розрахунку нелінійних перетворень блочних шифрів.

Об’єктом дослідження є процес обробки та перетворення даних для захисту інформації в комп'ютерних системах та мережах.

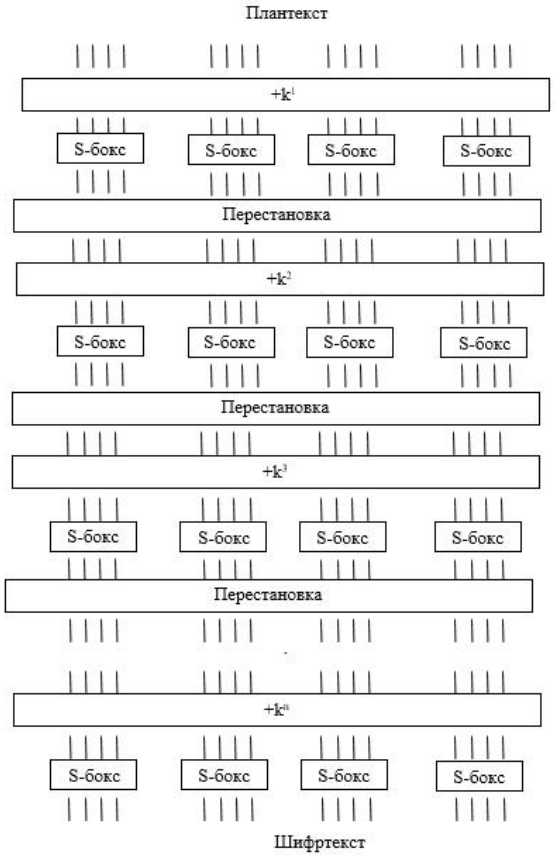
Предметом є методи формування нелінійних перетворень для шифрування, які реалізовані паралельним обчисленням.

Наукова новизна: вперше розроблено метод обчислення нелінійного перетворення, що складається з високонелінійних бульових функцій, який на відміну від існуючих використовує паралельну обробку, що дає можливість підвищити ефективність роботи в комп’ютерних системах та мережах за рахунок збільшення швидкодії реалізації.

Сучасні методи формування блочних шифрів



Мережа Фейстеля



Підстановочно-перестановочна мережа

Способи формування нелінійного перетворення (S-box):

Табличний (S-бокс DES)

	$b_2b_3b_4b_5$															
$b_1\ b_6$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	1	5	0	15	14	2	3	12

Алгебраїчний (S-бокс AES)

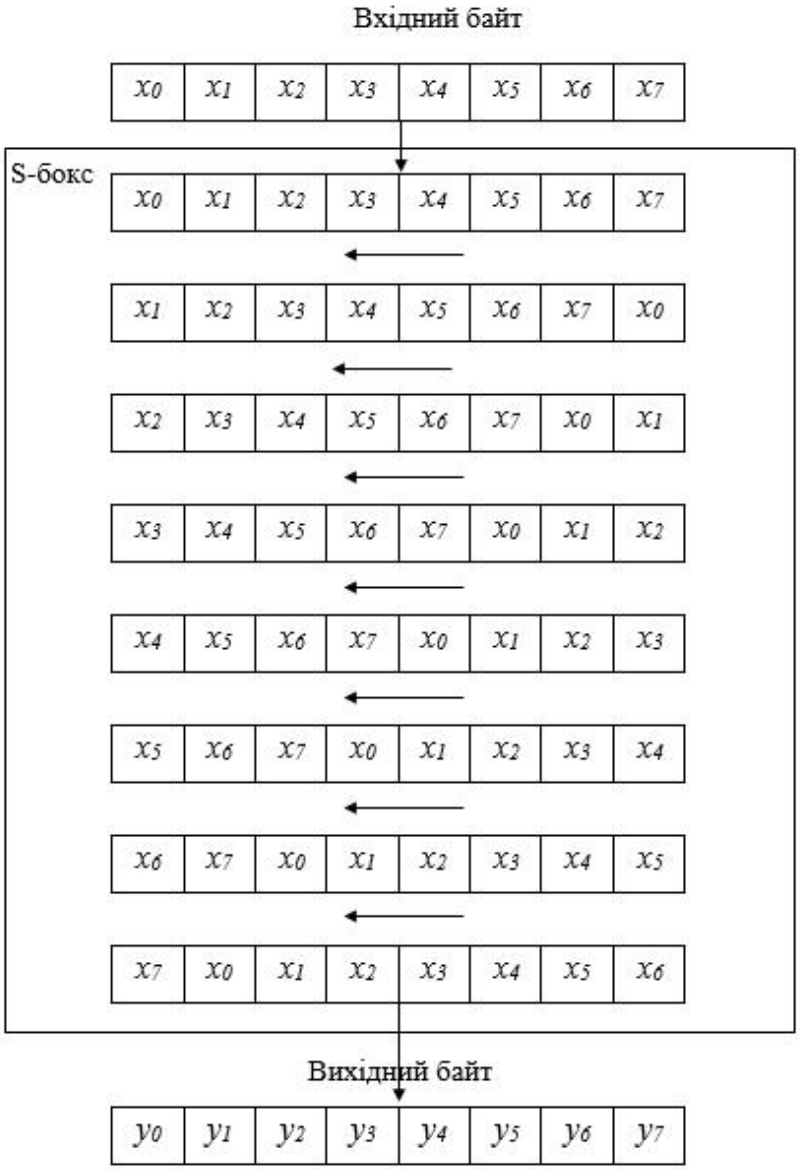
$$S = x^{-1} \bmod m(x) = x^8 + x^4 + x^3 + x + 1 \qquad (1)$$

де, $x \in GF(2^8)$

Метод формування S-боксу на основі високонелінійної булевої функції

Визначення аргументів функції
для розрахунку S-боксу

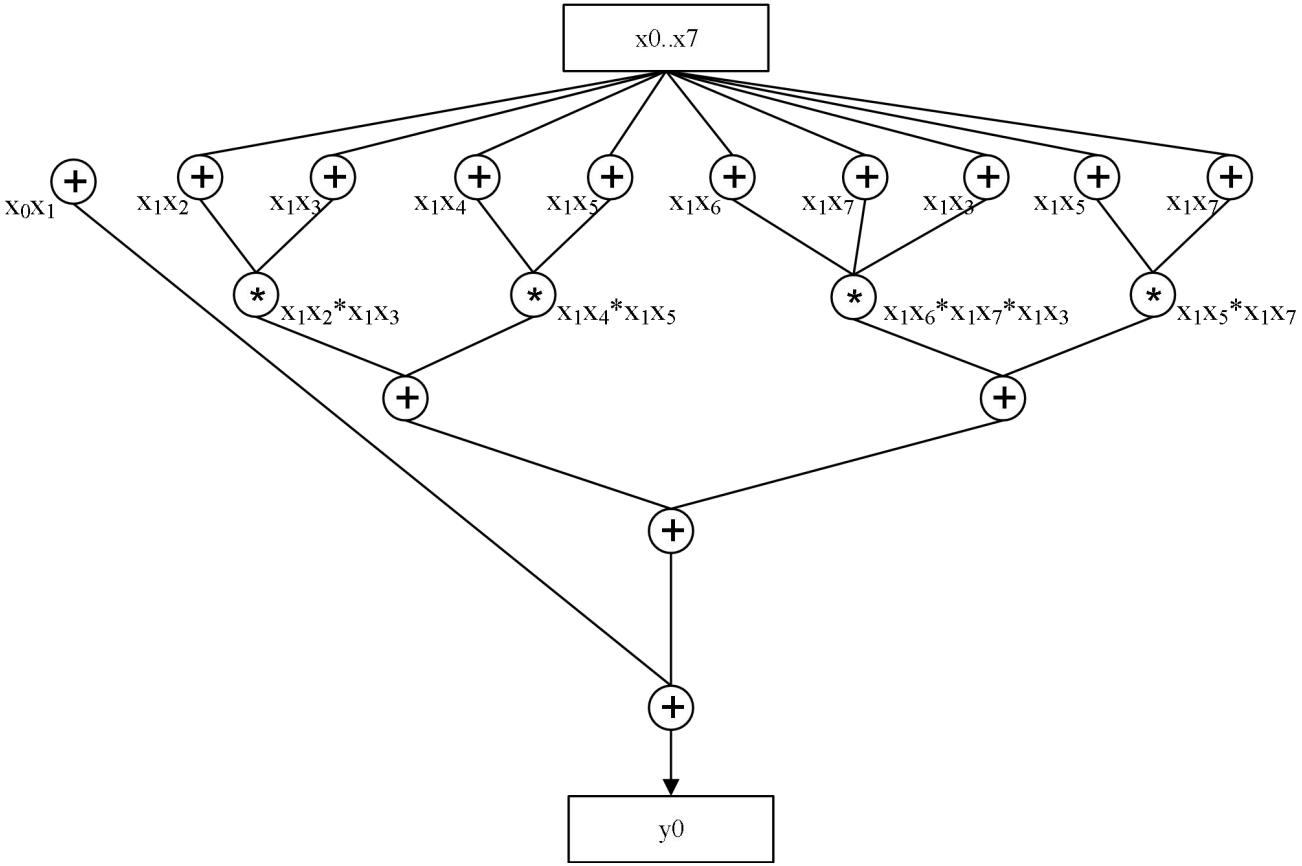
$$y = x_0 \oplus x_1 \oplus (x_1 \oplus x_2)(x_1 \oplus x_3) \oplus (x_1 \oplus x_4)(x_1 \oplus x_5) \oplus (x_1 \oplus x_6)(x_1 \oplus x_7) \oplus (x_1 \oplus x_3)(x_1 \oplus x_5)(x_1 \oplus x_7). \quad (2)$$


Вхідний байт
x0 x1 x2 x3 x4 x5 x6 x7
S-бокс
x0 x1 x2 x3 x4 x5 x6 x7
x1 x2 x3 x4 x5 x6 x7 x0
x2 x3 x4 x5 x6 x7 x0 x1
x3 x4 x5 x6 x7 x0 x1 x2
x4 x5 x6 x7 x0 x1 x2 x3
x5 x6 x7 x0 x1 x2 x3 x4
x6 x7 x0 x1 x2 x3 x4 x5
x7 x0 x1 x2 x3 x4 x5 x6
Вихідний байт
y0 y1 y2 y3 y4 y5 y6 y7

Розрахунок бітів результату S-боксу

$$
\begin{aligned}
y_0 &= x_0 \oplus x_1 \oplus (x_1 \oplus x_2)\,(x_1 \oplus x_3) \oplus (x_1 \oplus x_4)\,(x_1 \oplus x_5) \oplus (x_1 \oplus x_6)\,(x_1 \oplus x_7) \oplus (x_1 \oplus x_3)\,(x_1 \oplus x_5)\,(x_1 \oplus x_7).\\
y_1 &= x_1 \oplus x_2 \oplus (x_2 \oplus x_3)\,(x_2 \oplus x_4) \oplus (x_2 \oplus x_5)\,(x_2 \oplus x_6) \oplus (x_2 \oplus x_7)\,(x_2 \oplus x_0) \oplus (x_2 \oplus x_4)\,(x_2 \oplus x_6)\,(x_2 \oplus x_0).\\
y_2 &= x_2 \oplus x_3 \oplus (x_3 \oplus x_4)\,(x_3 \oplus x_5) \oplus (x_3 \oplus x_6)\,(x_3 \oplus x_7) \oplus (x_3 \oplus x_0)\,(x_3 \oplus x_1) \oplus (x_3 \oplus x_5)\,(x_3 \oplus x_7)\,(x_3 \oplus x_1).\\
y_3 &= x_3 \oplus x_4 \oplus (x_4 \oplus x_5)\,(x_4 \oplus x_6) \oplus (x_4 \oplus x_7)\,(x_4 \oplus x_0) \oplus (x_4 \oplus x_1)\,(x_4 \oplus x_2) \oplus (x_4 \oplus x_6)\,(x_4 \oplus x_0)\,(x_4 \oplus x_2).\\
y_4 &= x_4 \oplus x_5 \oplus (x_5 \oplus x_6)\,(x_5 \oplus x_7) \oplus (x_5 \oplus x_0)\,(x_5 \oplus x_1) \oplus (x_5 \oplus x_2)\,(x_5 \oplus x_3) \oplus (x_5 \oplus x_7)\,(x_5 \oplus x_1)\,(x_5 \oplus x_3).\\
y_5 &= x_5 \oplus x_6 \oplus (x_6 \oplus x_7)\,(x_6 \oplus x_0) \oplus (x_6 \oplus x_1)\,(x_6 \oplus x_2) \oplus (x_6 \oplus x_3)\,(x_6 \oplus x_4) \oplus (x_6 \oplus x_0)\,(x_6 \oplus x_2)\,(x_6 \oplus x_4).\\
y_6 &= x_6 \oplus x_7 \oplus (x_7 \oplus x_0)\,(x_7 \oplus x_1) \oplus (x_7 \oplus x_2)\,(x_7 \oplus x_3) \oplus (x_7 \oplus x_4)\,(x_7 \oplus x_5) \oplus (x_7 \oplus x_1)\,(x_7 \oplus x_3)\,(x_7 \oplus x_5).\\
y_7 &= x_7 \oplus x_0 \oplus (x_0 \oplus x_1)\,(x_0 \oplus x_2) \oplus (x_0 \oplus x_3)\,(x_0 \oplus x_4) \oplus (x_0 \oplus x_5)\,(x_0 \oplus x_6) \oplus (x_0 \oplus x_2)\,(x_0 \oplus x_4)\,(x_0 \oplus x_6).
\end{aligned}
\qquad (3)
$$

Обчислювальна модель алгоритму розрахунку результату S-боксу на основі даної булевої функції



Властивості розробленої обчислювальної схеми

Орієнтований ациклічний граф множини операцій для запропонованого обчислення

$$G = (V, R) \tag{4}$$

Множина для паралельної реалізації

$$H_p = \{(i, P_i, t_i) : i \in V\} \tag{5}$$

$\forall i, j \in V : t_i = t_j \Rightarrow P_i = P_j$ - умова 1. В один і той же момент часу не повинен призначатися різним операціям один і той же процесор;

$\forall (i, j) \in R \Rightarrow t_j \geq t_i + 1$ - умова 2. До призначеного моменту виконання операції всі необхідні розрахунки даних вже повинні бути обчислені.

Максимальний час паралельного виконання

$$T_p(G, H_p) = \max_{i \in V}(t_i + 1) \quad (6)$$

Мінімальний час виконання алгоритму

$$T_p(G) = \min_{H_p} T_p(G, H_p) \quad (7)$$

Нижній поріг мінімального часу тривалості алгоритму

$$T_p = \min_{G} T_p(G) \quad (8)$$

Прискорення при застосуванні *p* кількості процесорів

$$S_p(n) = T_1(n) / T_p(n) \quad (9)$$

Ефективність використання паралельного алгоритму

$$E_p(n) = T_1(n) / (pT_p(n)) = S_p(n) / p \quad (10)$$

Загальний час роботи алгоритму

$$T_p = 2\log_2 n, p = (n / \log_2 n) \quad (11)$$

Оцінка прискорення для розробленої графічної схеми та ефективності

$$S_p = T_1 / T_{pn} = (n-1) / 2\log_2 n \qquad (12)$$

$$E_p = T_1 / pT_p = (n-1)/(2n/\log_2 n)\log_2 n) = (n-1)/2n \qquad (13)$$

Отримані значення показника прискорення та ефективності паралельного обчислення

Значення прискорення для кожного рівня:

$$S_{p1} = 1.9342,\ S_{p2} = 1.5,\ S_{p3} = 1,\ S_{p4} = 1,\ S_{p5} = 0. \quad (14)$$

Значення ефективності для кожного рівня:

$$E_{p1} = 0.242,\ E_{p2} = 0.1875,\ E_{p3} = 0.125, E_{p4} = 0.125,\ E_{p5} = 0. \quad (15)$$

Крок підстановки

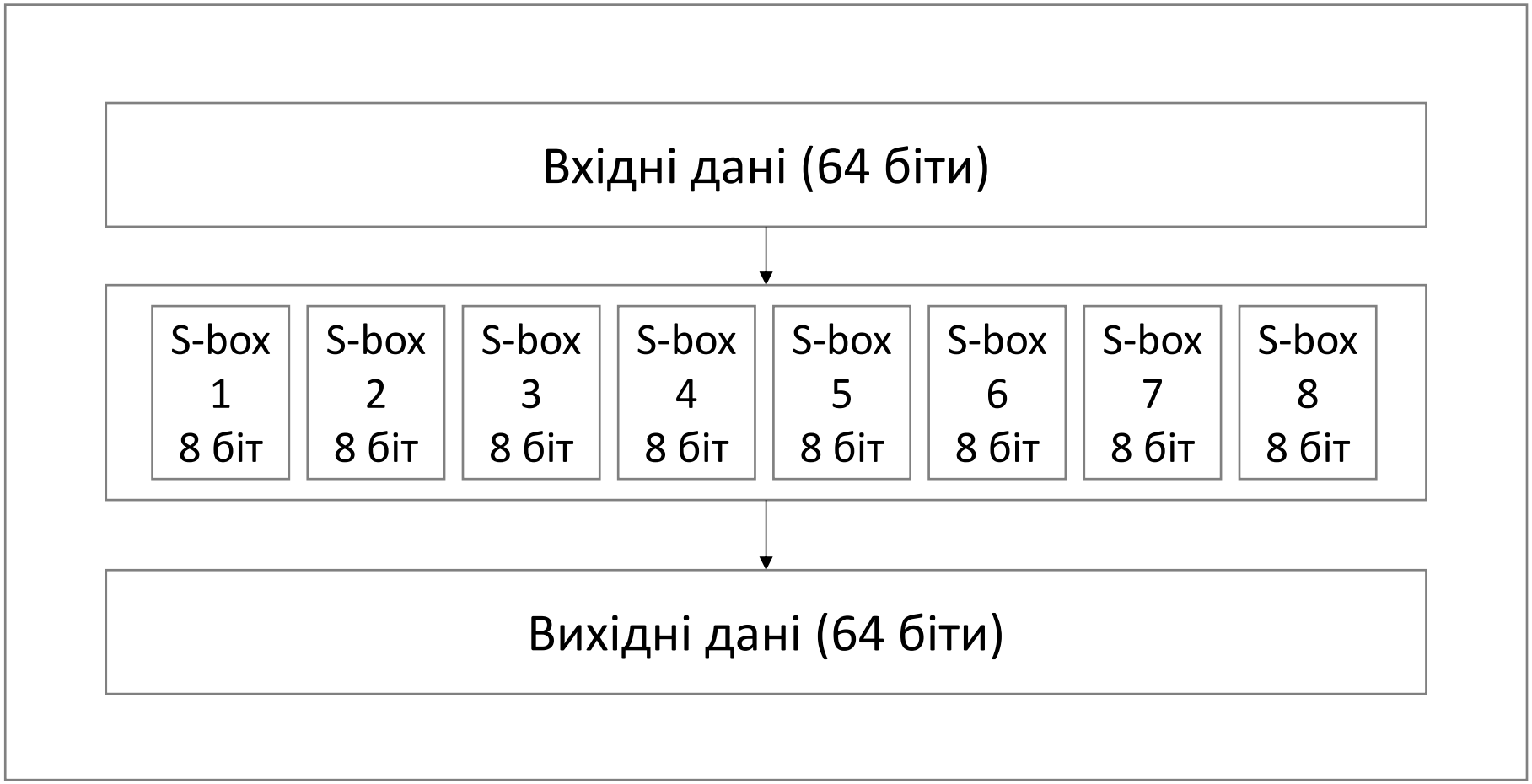
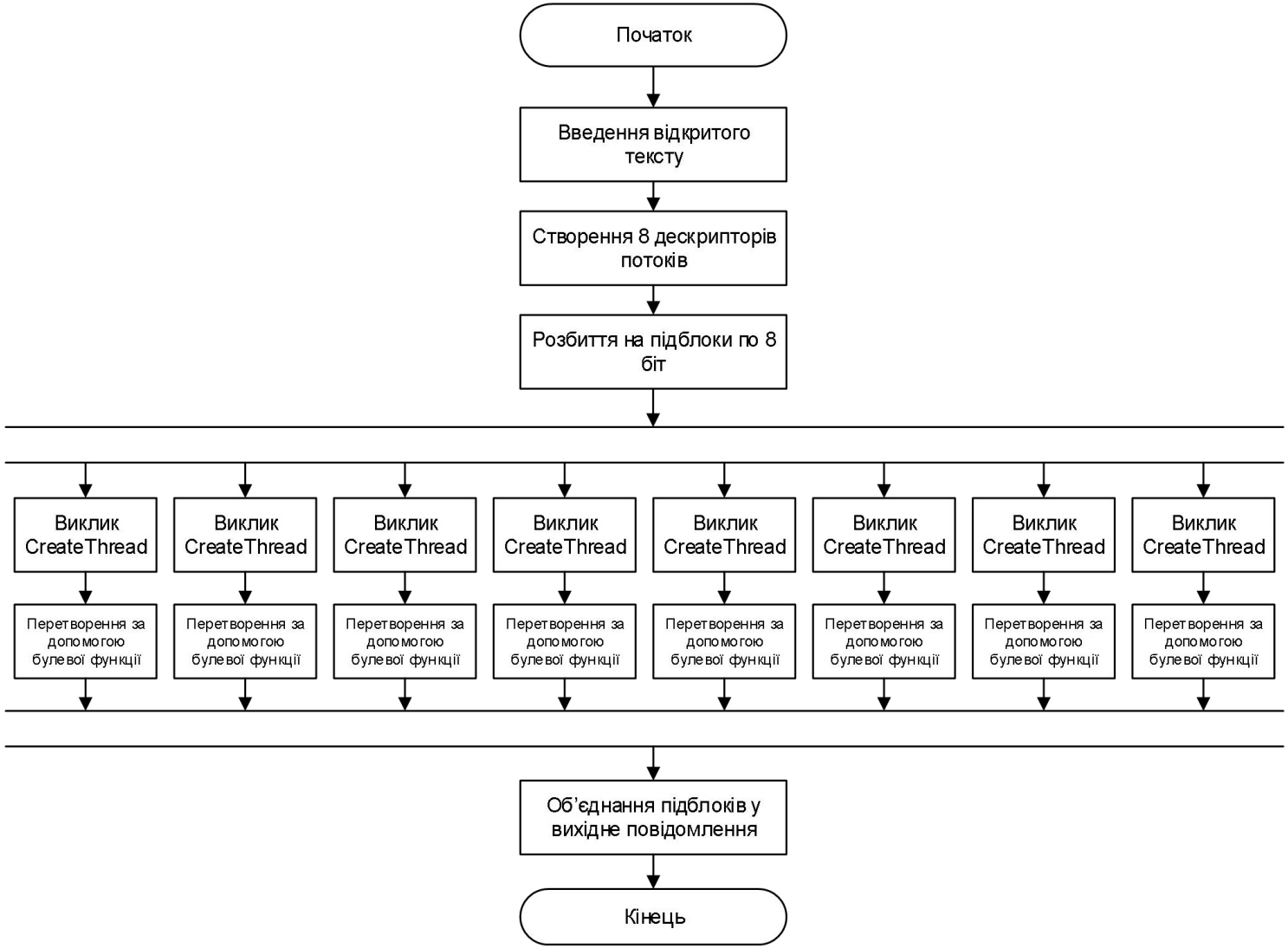


Схема програми



Експериментальне значення часу розрахунку S-боксу

№	Послідовний спосіб (мс)	Паралельний спосіб (мс)
1	10	5
2	11	6
3	9	7
4	8	7
5	10	5
6	9	6
7	8	7
Середнє значення	9,28	6,14

Висновки

В магістерській кваліфікаційній роботі виконано дослідження з метою підвищення швидкості реалізації захисту інформації в комп'ютерних системах та мережах на основі розробки нових методів та засобів паралельного обчислення результатів розрахунку нелінійних перетворень блочних шифрів.

Результатами досліджень є такі досягнення:

- створено метод паралельного обчислення нелінійного перетворення блочного шифру, в основі якого лежить високонелінійна бульова функція. Даний метод паралельного обчислення демонструє підвищення ефективності на 19-50%, а швидкість реалізації – на 50-90% в порівнянні з послідовним обчисленнням на комп’ютерній системі, яка буде складатися з одного процесора.
- на основі розробленого методу обчислення нелінійного перетворення блочного шифру розроблено програмний засіб, який виконує шифрування блоку даних розміру 64 біт. Швидкодія розробленого методу в 1,4 – 1,5 разів вище ніж у послідовного методу розрахунку нелінійного перетворення.