УДК 004.056 : 004.424.47

КОНСТРУКЦІЇ ГЕШУВАННЯ ІЗ ЗАВ'ЯЗУВАННЯМ БЛОКІВ ДАНИХ.

Слободян С. О.
Науковий керівник – к. т. н., ст. викл. Баришев Ю. В.

В роботі розглянуто конструкції Правіна Гауравара. Конструкція гешування з лінійною контрольною сумою. Вхідними значеннями до функції f(.) подаються значення масиву, та проміжне значення h_i, де h_0 задається ключовим. Функція виконує кількість проходів рівну довжині масиву повідомлення плюс один прохід. На додатковий прохід функції замість значення масиву подається контрольна сума розміру масиву повідомлення та проміжних значень h_i. Також в роботі розглянуті такі конструкції: 3С, ГОСТ-х та 3СА.

Метою дослідження є підвищення стійкості гешування до загальних атак.

Розглянуті підходи дещо ускладнює роботу зловмисника за рахунок введення додаткових обчислень на кожному з проміжних етапів, але не грають значної ролі в подоланні геш-атак загалом. Дані алгоритми гешування побудований лінійно, тому зловмисник, як і перед вдосконаленням функції має можливість реалізовувати загальні атаки.

Для покращення методів гешування необхідно подолати лінійність функцій у власної конструкції (рис. 1).

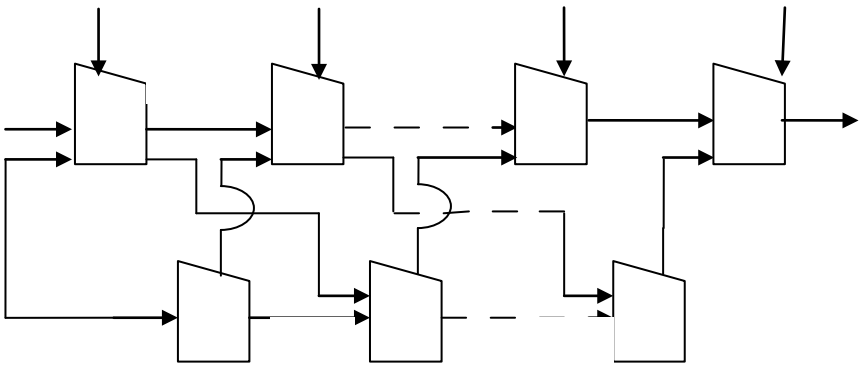

Рисунок 1– Конструкція гешування з лінійною контрольною сумою

На вхід функції подається значення елементів масиву, проміжних значень h_i та g_i.

В основі побудови нового методу лежить залежність проміжних геш-значень від певного виразу, що обчислюється на кожній ітерації, наприклад таке:

$$\begin{cases} h_i = f(h_{i-1}, g_{i-1}, m_i) \\ g_i = f^*(h_{i-2}, g_{i-1}) \end{cases}$$

В свою чергу значення g_i обчислюється для кожної ітерації окремо та формується із попередніх проходу g_{i-1} та h_{i-2}. Відповідно руйнується лінійність, що значно ускладнює роботу зловмисника.