УДК 681.3

ХЕШУВАННЯ ДАНИХ З НЕРІВНОМІРНИМ РОЗБИТТЯМ НА БЛОКИ

В.А. Лужецький, д.т.н., професор,
О.В. Філіппов, магістрант
Вінницький національний технічний університет
phil-oleg@ukr.net

Відомі методи хешування, які передбачають розбиття повідомлення (даних) на блоки однакової довжини і виконання певного фіксованого набору арифметичних і логічних операцій над цими блоками даних.

У доповіді розглядається новий підхід до хешування, який принципово відрізняється від усіх відомих методів хешування. Цей підхід полягає в тому, що розбиття початкового повідомлення здійснюється на блоки різної довжини і над кожним з блоків виконується своя специфічна послідовність операцій.

Для реалізації цього підходу пропонується метод хешування, який детально розглядається в доповіді.

Метод хешування:

1. Для поточного значення хеш-функції формуються ознаки розрядності поточного блоку даних і виконуваної операції.

2. Виконуються операції згідно з ознакою типу операції над поточним значенням хеш-функції і поточним блоком даних.

Пункти 1, 2 виконують певну кількість разів, яка визначається виходячи з ознаки розрядності блоку даних і розрядності хеш-значення.

Початкові дані мають вигляд $M = m_0 \| m_1 \| m_2 \| \ldots \| m_{N-1}$, де m_i – поточний блок даних певної розрядності.

У процесі хешування формується така послідовність хеш-значень $h_0, h_1, h_2, \ldots h_N$, де h_0 – початкове значення хеш-функції, h_N - результат хешування початкового повідомлення.

Нехай розрядність процесора l_{np}, тоді початкове і поточні значення хеш-функції розбиваються на підблоки довжиною l_{np}. Кількість таких підблоків дорівнює: $K = L_H / l_{np}$, де L_H – довжина хеш-значення.

Отже $h_i = h_{i,1} \| h_{i,2} \| \ldots h_{i,k}$, для $i = 0 \div (N-1)$

Ознака виконуваної операції формується як значення функції: $S_O = f(h_{i,k})$

Ознака розрядності блока даних визначається за формулою: $S_P = f^*(h_{i,(k-1)})$

Розрядність поточного блока даних дорівнює $l_i = (S_P + 1) \cdot l_{np}$,

Поточний блок даних розбивається на підблоки довжини l_{np}, тобто він представляється як конкатенація S_P підблоків $m_i = m_{i,1} \| m_{i,2} \| \ldots \| m_{i,(Sp+1)}$

Згідно з ознакою виконуваної операції здійснюється обчислення $h^{(g)}_{i,l} = h^{(g-1)}_{i,l} \overset{S_O}{\otimes} m_{i,g}$, де $g = 1 \div (S_P + 1)$, $l = 1 \div k$.

Поточне значення хеш-функції h_{i+1} формується як конкатенація результатів обчислень

$$h_{i+1} = h^{(Sp+1)}_{i,1} \| h^{(Sp+1)}_{i,2} \| \ldots \| h^{(Sp+1)}_{i,k}$$

Як операції для хешування пропонується використовувати бінарні операції: логічне додавання (OR), логічне множення (AND), додавання за модулем 2 (XOR), додавання за модулем $2^{l_{np}}$.

Блок повідомлення m_{N-1} у загальному випадку може мати розрядність, що відрізняється від розрядності, яка визначається ознакою, тому пропонується доповнювати блок до потрібної розрядності кодом числа N і певною кількістю розрядів псевдовипадкової послідовності.