УДК 004.056:004.424.47

МЕТОД ПРИШВИДШЕНОГО ХЕШУВАННЯ ДАНИХ

В. А. Лужецький, д.т.н. професор,
К. В. Черняхович, асистент,
І. В. Рудий, студент
Вінницький національний технічний університет

Метод хешування, який розглядається в доповіді, полягає в тому, що інформаційні дані подаються у вигляді послідовності блоків фіксованої розрядності:

$$M = m_1||m_2||m_3|| \dots ||m_N$$

і починаючи з деякого хеш-значення h_0, на кожній ітерації хеш-значення обчислюється за виразом:

$$h_i = g^{h_{i-1} \oplus m_i} (mod\ p),\ i = 1,2,3, \dots, N, \quad (1)$$

де g – примітивний елемент за модулем p;

p – просте число.

Результатом хешування є значення $\mathrm{h_N}$, отримане на останній ітерації.

Значення степеня $\mathrm{h_{i-1}} \oplus \mathrm{m_i}$ позначимо через $\mathrm{x = h_{i-1} \oplus m_i}$. Тоді формула (1) набуде вигляду:

$$h_i = g^x (mod\ p)$$

Представлення значення x у двійковій системі числення буде мати вигляд:

$$x = a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + a_{n-3}2^{n-3} + \dots + a_0.$$

Підставивши даний вираз в формулу (1) отримаємо:

$$h_i = g^{(a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + a_{n-3}2^{n-3} + \dots + a_0)} (mod\ p)$$

Застосовуючи математичні перетворення отримаємо:

$$h_i = g^{a_{n-1}2^{n-1}} \cdot g^{a_{n-2}2^{n-2}} \cdot g^{a_{n-3}2^{n-3}} \cdot \ldots \cdot g^{a_0} (mod\ p).$$

Даний вираз можна подати у вигляді:

$$h_i = (g^{2^{n-1}})^{a_{n-1}} \cdot (g^{2^{n-2}})^{a_{n-2}} \cdot (g^{2^{n-3}})^{a_{n-3}} \cdot \ldots g^{a_0}\ (mod\ p).$$

Значення $g^{2^{n-1}}, g^{2^{n-2}}, g^{2^{n-3}}, \ldots, g$ залишаються сталими на кожній ітерації хешування.

Пропонується попередньо обчислити значення цих сталих, зберігати їх в пам'яті обчислювального пристрою та використовувати при обчисленнях на кожній ітерації. У випадку коли $a_i = 0$, значення сталої g^{2^i} не враховується, тобто операція множення не виконується.

Під час виконання однієї ітерації хешування з використанням сталих g^{2^i}, необхідно виконати кількість операцій множення, яка визначається за виразом:

$$k_{бн} = n(v) - 1$$

де n - розрядність хеш-значення;

$n(v)$ – кількість одиниць у двійковому представленні x.

Для найскладнішого випадку $n = n(v)$ ефективність застосування попередніх обчислень, в порівнянні із застосуванням бінарного алгоритму піднесення до степеня в обчисленнях визначається за формулою:

$$E = \left(1 - \frac{n-1}{2(n-1)}\right)$$

Таким чином застосування попередніх обчислень при формуванні хеш-значення дозволяє пришвидшити процес хешування не менше ніж на 50%. Однак такий підхід вимагає додаткового об'єму пам'яті, яка використовується для зберігання значень констант g^{2^i}.