УДК 004.056:004.424.47

МЕТОД ХЕШУВАННЯ ДАНИХ НА ОСНОВІ МОДЕЛІ КВАТЕРНІОНА

Возний М.С.
Науковий керівник – проф., д.т.н. Лужецький В. А.

На даний час широко використовують хеш-функції за алгоритмами MD5 і SHA. Ці алгоритми забезпечують довжину хеш-значення 128 і 160 бітів відповідно. Було показано, що для такої розрядності можна знаходити колізії, тому висуваються вимоги до збільшення розрядності хеш-значення до 256 чи 512. Але такі розрядності вимагають складних обчислень і тому для хешування великих обсягів інформації потрібен великий час. З метою пришвидшення процесу хешування пропонується здійснювати обчислення кількох хеш-значень меншої розрядності з наступним їх об'єднанням в остаточний результат. Але такий підхід послаблює стійкість хеш-функції до колізій. Тому потрібно певним чином на кожному кроці хешування зав'язувати проміжні результати. Пропонується підхід, що передбачає зав'язування складових хеш-значення на основі моделі кватерніона.

Хеш-функція на основі математичної моделі множення кватерніонів буде представлена так: $h_i = f(h_{i-1}, m_i)$, де m_i – блок інформаційних даних (дані представляються у вигляді $M = \{m_1, m_2, \ldots, m_n\}$) , h_{i-1} – проміжне значення хеш-функції.

Значення h_{i-1} представляється у вигляді $h_{i-1} = \{a_{i-1}, b_{i-1}, c_{i-1}, d_{i-1}\}$, або у вигляді кватерніона:

$$h_{i-1} = a_{i-1} + b_{i-1}\mathbf{i} + c_{i-1}\mathbf{j} + d_{i-1}\mathbf{k}.$$

Блок даних m_i представляється у вигляді $m_i = \{e_i, f_i, g_i, u_i\}$, або:

$$m_i = e_i + f_i\mathbf{i} + g_i\mathbf{j} + u_i\mathbf{k}.$$

Тоді результат хеш-функції h_i представляється так:

$$h^*_i = h_{i-1}m_i = (a_{i-1} + b_{i-1}\mathbf{i} + c_{i-1}\mathbf{j} + d_{i-1}\mathbf{k})(e_i + f_i\mathbf{i} + g_i\mathbf{j} + u_i\mathbf{k}) =$$
$$= a_{i-1}e_i - b_{i-1}f_i - c_{i-1}g_i - d_{i-1}u_i + (a_{i-1}f_i + b_{i-1}e_i + c_{i-1}u_i - d_{i-1}g_i)\mathbf{i} +$$
$$+ (a_{i-1}g_i + c_{i-1}e_i + d_{i-1}f_i - b_{i-1}u_i)\mathbf{j} + (a_{i-1}u_i + d_{i-1}e_i + b_{i-1}g_i - c_{i-1}f_i)\mathbf{k},$$

або:

$$h_i = d\{a_i, b_i, c_i, d_i\},$$

де:

$$a_i = d(a_{i-1}e_i - b_{i-1}f_i - c_{i-1}g_i - d_{i-1}u_i),\ b_i = d(a_{i-1}f_i + b_{i-1}e_i + c_{i-1}u_i - d_{i-1}g_i),$$
$$c_i = d(a_{i-1}g_i + c_{i-1}e_i + d_{i-1}f_i - b_{i-1}u_i),\ d_i = d(a_{i-1}u_i + d_{i-1}e_i + b_{i-1}g_i - c_{i-1}f_i).$$

Функція $d(x)$ – додавання молодших і старших розрядів аргументу x за модулем 2^n.

Розглянутий метод хешування забезпечує потрібний рівень стійкості до колізій при підвищенні швидкості хешування за рахунок розпаралелення обчислень і меншої кількості обчислень на кожному кроці.