УДК 681.3.07

ПРИШВИДШЕННЯ ПРОЦЕСУ ОБЧИСЛЕНЬ ЗНАЧЕНЬ ГЕШ-ФУНКЦІЙ НА ОСНОВІ ВИКОРИСТАННЯ МОДЕЛІ КВАТЕРНІОНІВ

В. А. Лужецький, д. т. н., професор; Кобзар І. В.
Вінницький національний технічний університет
ivan-kobzar@mail.ru

Відомо, що для геш-функцій з теоретично доведеною стійкістю, їх стійкість або опір колізіям прямо пропорційний довжині значення. В той же час, чим більша розрядність геш-значення, тим більше обчислень необхідно виконати для його визначення, а тому ці обчислення вимагають достатньо багато часу. Збільшення розрядності мікропроцесорів дозволяє виконувати такі обчислення швидше. Однак, з іншого боку, воно і дозволяє зловмиснику швидше «зламати» геш-функцію, відповідно доводиться знову збільшувати розрядність геш-значення. Таким чином, покращення апаратури не обумовлює, в загальному випадку, збільшення швидкості обчислення геш-значення. Виходячи з цих міркувань, можна зробити висновок, що актуальною є задача побудови геш-алгоритмів, які б дозволяли підвищити швидкість обчислень без втрати стійкості геш-функції.

У доповіді розглядається побудова геш-функції в якій проміжні геш-значення і дані, що підлягають гешуванню, представляються у вигляді кватерніонів.

Більшість відомих підходів до побудови гешування «з нуля» базуються на конструкції, тобто математичній моделі, Меркля-Дамгаарда, яка описується формулою:

$$f\left(h_{i-1}, m\right)_i = h_i,$$

де h_{i-1} — проміжне геш-значення, отримане після і-ої ітерації гешування; m_i — і-й блок даних, що входить до складу повідомлення $M=\{m_1, m_2, ..., m_n\}$; $f()$ — деяка функція ущільнення, що реалізується за схемою, представленою на рис. 1.

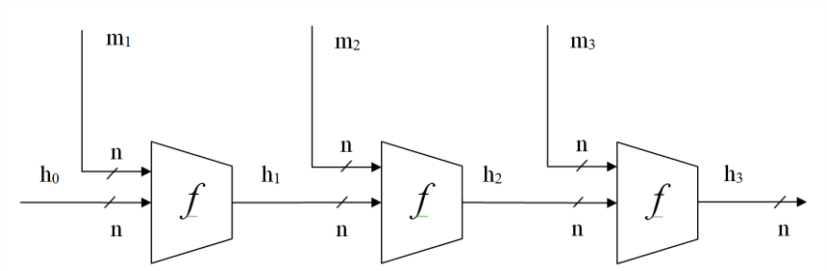

Рисунок 1 – Схема хешування

Вхідні значення h_{i-1} і m_i, розрядності n, розбиваються на 4 частини і представляються у вигляді кватерніонів, які розглядаються лише з цілочисельними координатами і мають вигляд:

$$q = a + bi + cj + dk,$$

де a,b,c,d — цілі числа; i,j,k — уявні одиниці, що задовольняють співвідношенням:

$$i^2 = j^2 = k^2 = i \cdot j \cdot k = -1$$

Тому представлення h_{i-1} і m_i у вигляді кватерніонів буде мати такий вигляд:

$$h_{i-1} = a_1 + b_1\, i + c_1\, j + d_1\, k$$

$$m_i = a_2 + b_2\, i + c_2\, j + d_2\, k$$

Відомо, що операція множення дозволяє забезпечити рівномірний вплив кожного біта на вихідне геш-значення, відповідно доцільно її використати для домішування результату обробки блоків даних до геш-значення, отриманого на попередній ітерації. Враховуючи це, пропонується визначити значення геш-функції як добуток вхідних елементів за модулем 2^n.

$$h_i = (h_{i-1} \cdot m_i) mod 2^n$$

При множенні кватерніонів враховуються такі правила множення їх елементів:

$$i^2 = j^2 = k^2 = -1$$
$$i \cdot j = k;\ j \cdot i = -k;$$
$$i \cdot k = j;\ k \cdot i = -j;$$
$$j \cdot k = i;\ k \cdot j = -i$$

Результат множення h_{i-1} на m_i буде мати такий вигляд:

$$\begin{aligned}
&\left((a_1 + b_1\, i + c_1\, j + d_1\, k) \cdot (a_2 + b_2\, i + c_2\, j + d_2\, k)\right) = \\
&= (a_1\, a_2 - b_1\, b_2 - c_1\, c_2 - d_1\, d_2) \\
&+ i(a_1\, b_2 + b_1\, a_2 + c_1\, d_2 - d_1\, c_2) \\
&+ j(a_1\, c_2 + c_1\, a_2 + b_1\, d_2 - d_1\, b_2) \\
&+ k(a_1\, d_2 + d_1\, a_2 + b_1\, c_2 - c_1\, b_2)
\end{aligned}$$

Кожен з добутків має розрядність $2n$. Нехай p_1 і p_2 числа що відповідають молодшим n-розрядам і старшим n-

розрядам добутку. Тоді функцію ущільнення усіх добутків можна представити як:

$$(p_1 + p_2) mod\, 2^n$$

З урахуванням, цього результат множення кватерніонів з ущільненням можна представити в такому вигляді:

$$\begin{aligned}
&\left((a_1 + b_1\, i + c_1\; j + d_1\, k)\cdot(a_2 + b_2\, i + c_2\; j + d_2\, k)\right) ущ. = \\
&= \left(P_{a_1 a_2} - P_{b_1 b_2} - P_{c_1 c_2} - P_{d_1 d_2}\right) mod 2^n \\
&+ i\left(P_{a_1 b_2} + P_{b_1 a_2} + P_{c_1 d_2} - P_{d_1 c_2}\right) mod 2^n \\
&+ j\left(P_{a_1 c_2} + P_{c_1 a_2} + P_{b_1 d_2} - P_{d_1 b_2}\right) mod 2^n \\
&+ k\left(P_{a_1 d_2} + P_{d_1 a_2} + P_{b_1 c_2} - P_{c_1 b_2}\right) mod 2^n
\end{aligned}$$

Відомі геш-фунції теоретично-доведеної стійкості які використовують операції піднесення до степеня. Якщо таку функцію реалізувати з використанням 4 каналів розрядності n, то в середньому буде потрібно виконати 1,5n операцій множення на кожній ітерації для одного каналу, або 6n операцій множення для 4 каналів. Для обчислення геш-значення за алгоритмом що пропонується потрібно виконати 16 операцій множення і 28 операцій додавання на кожній ітерації. У сучасних мікропроцесорах операція додавання і множення виконується приблизно за однаковий час, тому буде потрібно виконати 44 операції.

Нехай розрядність геш-значення 256, тоді n=64. У відомому випадку буде потрібно 384 операції на кожній ітерації, тому пришвидшення складає 8.7 рази.