УДК 004.056:004.424.47

МЕТОД ХЕШУВАННЯ ДАНИХ ШЛЯХОМ РОЗПАРАЛЕЛЕННЯ ОБЧИСЛЕНЬ І ЗАВЯЗУВАННЯМ ПРОМІЖНИХ РЕЗУЛЬТАТІВ

В. А. Лужецький, д.т.н., професор,
М. С. Возний, бакалавр з інформаційної безпеки
Вінницький національний технічний університет

Одним із підходів забезпечення стійкості хешування є збільшення розрядності проміжних хеш-значень. Але отримання хеш-значень великої розрядності вимагає 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. В доповіді розглядається підхід, що передбачає зав'язування складових хеш-значення з використанням вектора керування.

Математична модель хеш-функції представляється так:

$$h_i = f(h_{i-1}, m_i, \nu_i),$$

де m_i – блок інформаційних даних (дані представляються у вигляді $\mathbf{M} = \{m_1, m_2, ..., m_k\}$), h_{i-1} – проміжне значення хеш-функції, ν_i – вектор керування, h_0 – початкове значення, h_k – результуюче хеш-значення.

Попередній результат хешування і блок інформаційних даних розбиваються на n підблоків, які

завязуються між собою для формування наступного хеш-значення.

Значення h_{i-1} представляється у вигляді набору значень блоків:

$$h_{i-1} = \{h_{i-1}^{(1)}, h_{i-1}^{(2)}, \ldots, h_{i-1}^{(n)}\},$$

Блок даних m_i представляється у вигляді набору значень підблоків:

$$m_i = \{m_i^{(1)}, m_i^{(2)}, \ldots, m_i^{(n)}\},$$

Тоді результат хешування h_i представляється як набір значень підблоків:

$$h_i = \{h_i^{(1)}, h_i^{(2)}, \ldots, h_i^{(n)}\},$$

Необхідно, щоб кожен підблок мав однаковий вплив на результат. Для цього кожен підблок попереднього хеш-значення завязується з кожним підблоком інформаційних даних. Підблоки завязуються між собою в n каналах, обчислення в яких здійснюються паралельно. Оскільки один підблок попереднього хеш-значення завязується з кожним з n підблоків інформаційних даних, то утворюється n обчислювальних каналів:

$$h_i^{(1)} = h_{i-1}^{(1)} \circledast m_i^{(1)} \odot h_{i-1}^{(2)} \circledast m_i^{(2)} \odot \ldots \odot h_{i-1}^{(n)} \circledast m_i^{(n)},$$
$$h_i^{(2)} = h_{i-1}^{(1)} \circledast m_i^{(2)} \odot h_{i-1}^{(2)} \circledast m_i^{(3)} \odot \ldots \odot h_{i-1}^{(n)} \circledast m_i^{(1)},$$
$$\ldots$$
$$h_i^{(n)} = h_{i-1}^{(1)} \circledast m_i^{(n)} \odot h_{i-1}^{(2)} \circledast m_i^{(1)} \odot \ldots \odot h_{i-1}^{(n)} \circledast m_i^{(n-1)},$$

де $\circledast$, $\odot$ – певні операції.

Результат хешування h_i отримується шляхом конкатенації результатів виконання операцій в кожному з каналів.

Для забезпечення стійкості хеш-значення пропонується, щоб в кожному каналі, на кожній ітерації хешування операції між підблоками змінювались. Пропонується використовувати вектор керування для визначення операцій між підблоками.

Вектор керування генерується для кожної ітерації хешування. Вектор керування ν_i можна представити як конкатенацію n блоків. Кількість блоків залежить від кількості каналів, а розрядність кожного блоку від кількості операцій між підблоками і від кількості розрядів, що кодують одну операцію.

Пропонується два підходи для генерації вектора керування: з використанням попереднього результату хешування та без використання попереднього результату хешування.

Один із можливих варіантів генерування вектора керування із попереднього хеш-значення представлено на рис. 1.

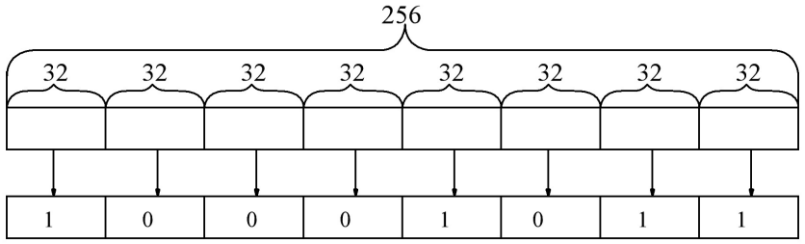

Рисунок 1 – Схема формування вектора керування за попереднім хеш-значенням

На рис. 1 наведено приклад формування вектора керування за попереднім хеш-значенням розрядності 256, що обчислюється в чотирьох каналах. В кожному каналі

використовується дві операції, які кодуються відповідно ‘0’ і ‘1’. Тому щоб закодувати всі операції в усіх каналах необхідний 8-ми розрядний вектор керування. В кожній 32-ох розрядній частині підраховується кількість одиниць. Якщо ця кількість парна, то у вектор керування записується ‘1’, якщо непарна – то ‘0’.

Інший підхід до формування вектора керування базується на використанні стану регістра зсуву зі зворотнім зв’язком. Можна весь стан регістра поміщати в вектор керування, а можна використовувати лише певні його розряди (рис. 2). При такому підході вектор керування буде незалежним від попереднього хеш-значення.

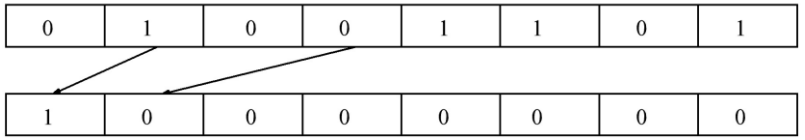

Рисунок 2 – Схема формування вектора керування за станом регістра зсуву

На рис. 2 з 8-ми розрядного регістра зсуву лише 2 і 4 розряди поміщаються у вектор керування.

В якості операцій для зав’язування підблоків пропонується використовувати такі операції:

- бінарні операції: $\oplus, \vee, \wedge$;
- додавання за модулем 2^m, множення за модулем 2^m.

Розглянутий метод хешування забезпечує потрібний рівень стійкості до колізій при підвищенні швидкості хешування. Програмна реалізація хеш-функції на основі даної моделі обробляє 512 бітів інформаційних даних на 32-х розрядному процесорі за 136 операцій (256 розрядне хеш-значення), програмна реалізація хеш-функції MD5 за 532 операції (128 розрядне хеш-значення).