УДК 004.056

# МЕТОД ХЕШУВАННЯ ІЗ ПСЕВДОВИПАДКОВОЮ ВИБІРКОЮ БЛОКІВ ДАНИХ

**В. А. Лужецький, д.т.н., професор**
**М. С. Гадалін, бакалавр з інформаційної безпеки**
**Вінницький національний технічний університет**
**mikle77g50@gmail.com**

Пропонується метод хешування даних, в якому передбачено розпаралелення обчислень і пропонується функцію ущільнення реалізовувати на основі правил додавання (віднімання) кодів Фібоначчі.

Вхідне повідомлення *M* розбивається на *n* блоків однакової довжини:

$$M = \{m_1, m_2, \dots, m_n\}.$$

Далі формується дві послідовності блоків за таким правилом. Відповідно до послідовності блоків повідомлення *M* формується послідовність 0 та 1 за допомогою генератора псевдовипадкових послідовностей (ГПВП). Якщо блоку $m_i$ відповідає символ 0, то цей блок входить до складу послідовності $M^0$, а якщо цьому блоку відповідає символ 1, то він входить до складу послідовності $M^1$:

$$M^0 = \{m^0_1, m^0_2, \dots, m^0_k\};$$

$$M^1 = \{m^1_1, m^1_2, \dots, m^1_r\};$$

$$k + r = n\ .$$

Операції хешування виконуються паралельно для послідовностей $M^0$ та $M^1$. Тому використовуються два

початкових хеш-значення:

$$h_0^0 = \{h^0{}_{01}, h^0{}_{02}, \dots, h^0{}_{0b}\};$$
$$h_0^1 = \{h^1{}_{01}, h^1{}_{02}, \dots, h^1{}_{0b}\},$$

де $b$ – кількість блоків хеш-значення;

$h_0^0$ – початкове хеш-значення для послідовності $M^0$;

$h_0^1$ – початкове хеш-значення для послідовності $M^1$.

Для формування поточного хеш-значення використовується функція ущільнення, аргументами якої є попереднє хеш-значення та поточне значення блоку даних:

$$M_i^0 = \{m^0{}_{1i}, m^0{}_{2i}, \dots, m^0{}_{bi}\};$$
$$M_i^1 = \{m^1{}_{1i}, m^1{}_{2i}, \dots, m^1{}_{bi}\}.$$

Результат цієї функції циклічно зсувається вліво на $c$ блоків:

$$h_i^g = f_z\left(h_{i-1}^g, M_i^g\right) <<< c,$$

де $g = \{0,1\}$; $z = \{0,1\}$.

Значення $z$ вказує правило, яке описує функцію ущільнення. Якщо $z$=0, то це означає, що функція ущільнення описується правилом додавання кодів Фібоначчі, і при цьому наступне проміжне хеш-значення описується виразом:

$$h_i^g = h_{i-1}^g \overset{F}{\bigoplus} M_i^g,$$

де $\overset{F}{\bigoplus}$ – операція додавання кодів за правилами додавання кодів Фібоначчі.

У разі $z$=1 використовується правило віднімання кодів Фібоначчі:

$$h_i^g = h_{i-1}^g \ominus^F M_i^g ,$$

де $\ominus^F$ – операція віднімання кодів за правилами віднімання кодів Фібоначчі.

Значення $c$ визначається як сума одиниць попереднього хеш-значення за модулем $b$:

$$c = S(h_{i-1}^g) mod\ b ,$$

де $S$ – функція визначення суми одиниць попереднього хеш-значення.

На початку хешування $z$=0 для послідовності $M^0$ і $z$=1 для послідовності $M^1$.

Операція додавання кодів, що виконується за правилами додавання кодів Фібоначчі поширює у результуючому коді 1. Операція віднімання кодів, що виконується за правилами віднімання кодів Фібоначчі – 0.

Тому для рівномірного розподілу 0 та 1 в коді хеш-значення значення $z$ змінюється на протилежне після кожної ітерації хешування для обох послідовностей $M^0$ та $M^1$. Додавання і віднімання кодів за правилами додавання і віднімання кодів Фібоначчі забезпечує зав'язування кодів повідомлення і проміжного хеш-значення на бітовому рівні. Графічне зображення ітерації хешування наведено на рис. 1. Після завершення останньої ітерації хешування і отримання хеш-значень

$$h_N^0 = \{h^0{}_{N1}, h^0{}_{N2}, \dots, h^0{}_{Nb}\},$$

$$h_N^1 = \{h^1{}_{N1}, h^1{}_{N2}, \dots, h^1{}_{Nb}\}$$

виконуються такі операції:

$$H^0 = h_n^0 \overset{F}{\bigoplus} h_n^1;$$

$$H^1 = h_n^0 \ominus^F h_n^1;$$

$$H = H^0 \oplus H^1,$$

де $H$ – результуюче хеш-значення.

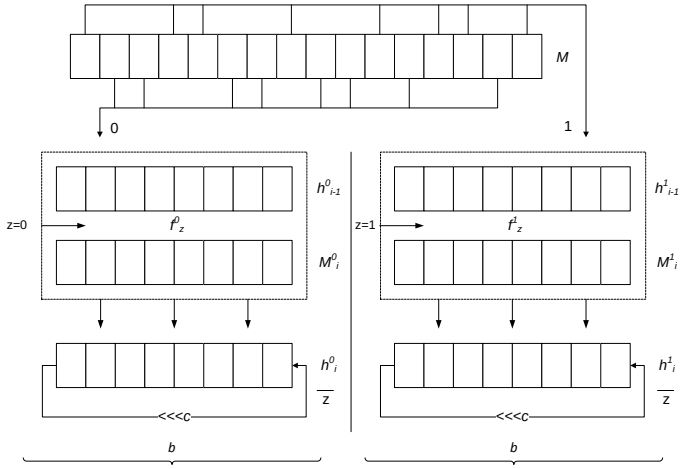


Рисунок 1 – Графічне зображення ітерації хешування

Використання псевдовипадкової вибірки даних забезпечує підвищення стійкості хеш-функції до атак.

Запропонований метод хешування може бути реалізований як безключове так і ключове хещування. Якщо початковий стан і поліном, який описує побудову ГПВП, відомі, то реалізується безключове хешування. Для ключового хешування як секретний ключ використовується код, що складається з коду початкового стану ГПВП та коефіцієнтів полінома.