УДК 004.056 : 004.424.47

АДАПТИВНИЙ МЕТОД ФОРМУВАННЯ ВЕКТОРІВ КЕРУВАННЯ ДЛЯ ХЕШУВАННЯ ДАНИХ

[1]Ю. В. Баришев, асистент;
[2]О. В. Оводенко, к. т. н., доцент
[1]Вінницький національний технічний університет
[2]Донецький національний технічний університет
yuriy.baryshev@gmail.com

Функціонування сучасних комп'ютерних систем передбачає передавання даних між робочими станціями та серверами. При цьому розв'язання задач перевірки автентичності даних та сторін, які приймають участь в обміні даних, набуває актуальності. Для розв'язання даних задач у комп'ютерних системах використовуються методи хешування (hashing). Водночас, відповідно до сучасних течій у криптології, алгоритми, за якими реалізується процес хешування, є відкритими. Більше того, вони передбачають ітеративне повторення певних перетворень відповідно до конструкцій хешування. Прикладом таких конструкцій є конструкція Меркля-Дамгаарда:

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

де h_i – проміжне хеш-значення, отримане після завершення обробки i-го блоку даних m_i $\left(i = \overline{1,l}\right)$; h_0 – вектор ініціалізації (частина ключа при ключовому варіанті хешування); $f(\cdot)$ – функція ущільнення.

Основним недоліком хешування, яке базується на конструкції (1) є можливість реалізації загальних атак, які не враховують перетворення, що реалізують функцію ущільнення $f(\cdot)$. Уникнути ітеративності перетворень

дозволяє концепція керованого хешування, при використання якої формула (1) набуває такого вигляду:

$$h_i = f_{v_i}(h_{i-1}, m_i), \qquad (2)$$

де v_i – вектор керування $v_i = g(a_1, a_2, ..., a_k)$, де a_j – j-й аргумент функції формування вектора керування $g(\cdot)$, причому $\sum_{j=1}^{k} \|a_j\| \geq \|v_i\|$ ($\|x\|$ – довжина x у бітах).

Оскільки функція ущільнення з керованими параметрами $f_{v_i}(\cdot)$ може мати довільну кількість керованих параметрів, тому доцільно, щоб метод формування вектора керування дозволяв отримувати вектори v_i довільної довжини. Для цього пропонується метод, який передбачає такі дії:

- об'єднання за допомогою конкатенації у блоки по l аргументів, де l – мінімальне ціле число, для якого виконується умова $\sum_{j=1}^{l} \|a_j\| \geq \|v_i\|$;

- останній блок формується шляхом конкатенації останніх $k \bmod l$ аргументів;

- отримані блоки додаються за модулем 2;

- результат додавання за модулем 2, розбивається на дві частини довжиною $\|v_i\|$ та $\sum_{j=1}^{l} \|a_j\| - \|v_i\|$ відповідно, які додаються за модулем 2.

Запропонований метод не залежить від конкретних довжин аргументів формування векторів керування, тому може бути використаний у методах керованого хешування, що передбачають використання декількох функцій ущільнення з керованими параметрами або адаптування до різних обчислювальних платформ.