УДК 004.056

АНАЛІЗ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ ДЛЯ КЕРОВАНОГО ГЕШУВАННЯ

Ю. В. Баришев, к.т.н., ст. викладач, В. І. Заглада
Вінницький національний технічний університет
yuriy.baryshev@gmail.com

З появою нових атак на алгоритми гешування виникає необхідність в перегляді створення функцій ущільнення, а також самих алгоритмів хешування. Один з можливих варіантів удосконалення гешування, який буде стійким до нових атак, є кероване гешування. Суть керованого хешування полягає у зміні використовуваних параметрів у функції ущільнення на протязі кожної ітерації.

Для створення ефективного та стійкого алгоритму керованого хешування необхідно розглянути та проаналізувати роботи, які вже були створені у даному напрямку.

В. Г. Бабенко, С. В. Рудницький пропонують метод захисту інформації на основі матричних операцій криптографічного перетворення. Суть даної моделі полягає у використанні матриці, яка формується на основі певного введеного ключа. Недолік даної моделі – обмеження, які накладає матриця: матриця не повинна мати нульові рядки, чи нульові стовбці; у матриці відсутні однакові рядки; сума за модулем два двох чи декількох рядків не повторює існуючий рядок матриці.

А. О. Бойко пропонує універсальні функції гешування на основі обчислення значення полінома в кільцях цілих чисел за модулем 2^n. На основі функції

PolyCW можливо побудувати інші функції гешування вибором інших модулів перетворень з простих чисел:

$$g_x(m) = \sum_{i=1}^{k} m_i \cdot x^i \bmod p$$

Дана ідея має свої недоліки: значення ключа з множини непарних чисел; парні значення повідомлень; зменшення розмірів простору ключів; геш-значення «не чутливе» до наявності нульових блоків даних в кінці повідомлення.

Відомий метод паралельного гешування, який передбачає введення залежностей операцій, які виконуються під час ітерації від вектора керування. В даній доповіді авторами пропонується розвиток цього підходу. У функції ущільнення використовується три параметри, а саме проміжне геш-значення, блок даних та вектор керування:

$$\begin{cases} h_i^{(j)} = f_{v_i^{(j)}}\left(h_{i-1}^{(j)}, m_i, v_i^{(j+1)}\right) \\ v_i^{(j)} = g\left(h_0^{(j)}, h_1^{(j)}, \ldots, h_{i-1}^{(j)}\right) \end{cases},$$

де $h_i^{(j)}$ - проміжне геш-значення; m_i $_{\text{i}}$- і-ий блок даних; $f(\bullet)$ - функція ущільнення; v_i - вектор керування; $g(\bullet)$ - функція формування вектора, керування.

Розроблено функції ущільнення, яка складається з двох виразів. Функція виконує один з заданих виразів на основі вектору керування.

$$f_{v_i}^{(j)} = \begin{cases} (\sim)(h_{i-1}^{(j)} >>> u_i) \cup (m_i \oplus v_i^j) \\ (h_{i-1}^{(j)} >>> u_i) \oplus m_i \end{cases},$$

де u_i - частина вектора керування.

В подальшому планується розробка програмного засобу та оцінка нелінійності перетворень.