УДК 004.424.47

МЕТОДИ КЛЮЧОВОГО ХЕШУВАННЯ ТЕОРЕТИЧНО ДОВЕДЕНОЇ СТІЙКОСТІ

Семененко Д.С.
Науковий керівник – аспірант Баришев Ю.В.

Сьогодні на практиці вирішується низка задач за допомогою хешування. Не для всіх з них час є критичним, зокрема задача перевірки цілісності банку данних, що не часто змінюються, як, наприклад, база даних відділу кадрів підприємства. Для такого класу задач вимога стійкості є важливішою, ніж вимога швидкості хешування.

Найбільш розповсюдені хеш-функції в наш час не гарантують стійкість. Це пов'язано з тим, що вони перевіряються на стійкість до відомих атак, що з'являються. А статистичні дослідження мають на меті перевірити наближенність результатів хешування до рівномірного розподілу. Останнє також не може гарантувати стійкість до нових атак. Відповідно є актуальною задача розробки методів хешування, доведення стійкості яких буде теоретичним.

В доповіді пропонується використовувати для хешування математичні задачі теоретично доведенної складності або такі, що є загальновизнанно складними. У межах даної доповіді розглядається задача дискретного логарифмування в полі простого числа, зокрема піднесення до степеня примітивного елемента за модулем та задача пошуку скалярного множника для точок еліптичної кривої.

Процес хешування теоретично доведенної стійкості, що використовує операцію піднесення до степеня за модулем, відбувається відповідно формули:

$$h_i = g^{h_{i-1}+m_i} \bmod p,$$

де p – велике просте число; m_i – і-тий блок данних (i=1,2,.., t); h_i – проміжне хеш-значення; g – примітивний елемент за модулем p.

Процес хешування, що базується на задачах пошуку скалярного множника для точок еліптичної кривої буде виконуватись відповідно формули:

$$h_i = m_i h_{i-1},$$

де $\{h_i\}$- точки еліптичної кривої.

Отже, в данній доповіді було наведено приклади реалізації методів хешування теоретично доведенної стійкості, що можуть гарантувати заданий рівень стійкості, хоча він є дещо нищим, ніж того вимагають від ідеальної хеш-функції.