УДК 003.26 : 004.424.47

МЕТОДИ ХЕШУВАННЯ З ПІДВИЩЕНОЮ СТІЙКІСТЮ ДО АТАК

Стах О. С.
Науковий керівник – аспірант Баришев Ю. В.

На даний момент ще не знайдено хешування, що наближається до ідеального. Більшості відомих алгоритмів хешування загрожують певні універсальні атаки, що використовують властивості конструкцій, зокрема до таких атак належать атаки Жукса, Келсі-Кохно. Суть атаки Жукса полягає у пошуку мультиколізій для функцій хешування, що обчислюються паралельно. Якщо розглянути дві такі функції, що мають вихідне значення розрядністю n, то згідно парадоксу дня народження, пошук 2^t колізій можна здійснити за $t \cdot 2^{n/2}$ підстановок. Серед 2^t колізій з великою ймовірністю знайдеться така, яка буде колізією і для іншої функції. Ідея атака Келсі-Кохно полягає в передобчисленні більшості можливих блоків даних і проміжних значень функції хешування. Якщо даний листок дерева був обчислений раніше, то його обробка припиняється. У даній атаці можна оптимально розділити використаний час та пам’ять, оскільки між ними існує лінійна залежність. Виходячи з цих міркувань, можна зробити висновок, що актуальною є побудова конструкції хешування з підвищеною стійкістю до атак.

Розглянемо алгоритм хешування теоретично доведеної стійкості, який використовую операцію піднесення до степеня за модулем простого числа. При виконанні даної операції для чисел великої розрядності неможливо визначити аргументи за реальний час, знаючи її результат. За основу піднесення до степеня візьмемо примітивний елемент за модулем. Пропонується як степінь взяти суму попередньої ітерації хешування та блоків даних, індекси яких змінюються на константи та на деяке згенероване псевдовипадкове число. Генерацію псевдовипадкого числа можна реалізувати лінійним конгруентним методом, що залежить від поточного блоку даних.

$$H_i = G^{H_{i-1}+m_{i-a}+m_{i-b}+m_{i-u_i}} \bmod p$$

де G – примітивний елемент; m_i – i-й блок даних; p – просте число.

Дана формула унеможливлює запис системи рівнянь через присутність псевдовипадкого індексу. Неможливо також вивести закономірність для перестановки індексів через константи. Легко бачити, що введення псевдовипадкового індексу на час хешування суттєво не вплине. Отже, було досягнуто суттєвого підвищення стійкості до атак без значної втрати в швидкості хешування.