УДК 004.056

РОЗРОБКА ШВИДКОДІЮЧИХ І ЗАХИЩЕНИХ ХЕШ-ФУНКЦІЙ

Очеретний Е. А.
Науковий керівник – доц., к. т. н. Семеренко В. П.

На теперішній час актуальна проблема розробки швидкодіючих і надійних хеш-функцій. Відомі потокові і блокові алгоритми хешування мають певні недоліки: блокові, при високому рівні захисту, працюють дуже повільно, а потокові не досить захищенні. В цій роботі проаналізовано існуючі методи хешуваня, та запропоновано метод хешування, що базується на роботі спеціального класу автоматів - лінійної послідовнісної машини.

За основу було взято вже існуючий метод сигнатурного аналізу, який використовується в тестуванні апаратних схем вже десятки років. Сигнатурний аналіз дуже схожий за своєю природою на хешування. Тому можна використати цей математичний апарат при розробці хеш-функцій.

Сигнатурний аналіз використовує так званні сигнатури - цифрові послідовності на певних виходах пристрою, які утворюються при подачі на вхід схеми тестової послідовності X. В роботі доведено, що сигнатура відповідає всім вимогам. які пред'являються до хеш-функції:

1) стійкість до колізій (два різні набори даних повинні мати різні результати перетворення);

2) необоротність (неможливість обчислення вхідних даних за результатом перетворення).

3) Зміна хоча б одного біта вхідної послідовності приводить до повної зміни вихідної послідовності;

4) швидкий алгоритм обчислення.

Для забезпечення криптостійкості хеш-функції на основі ЛПМ необхідно до отриманої сигнатури додати ключову послідовність k не менше 128 символів перед початком і після закінчення вхідної послідовності X (рис 1).

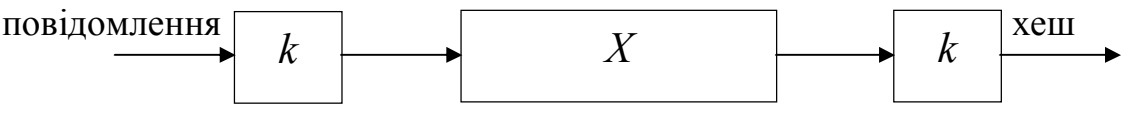

Рис.1 Реалізація захисту хеш-функції

Таким чином ці дві ключові послідовності відіграють роль секретного ключа і забезпечують необхідний рівень захисту хеш-функції.